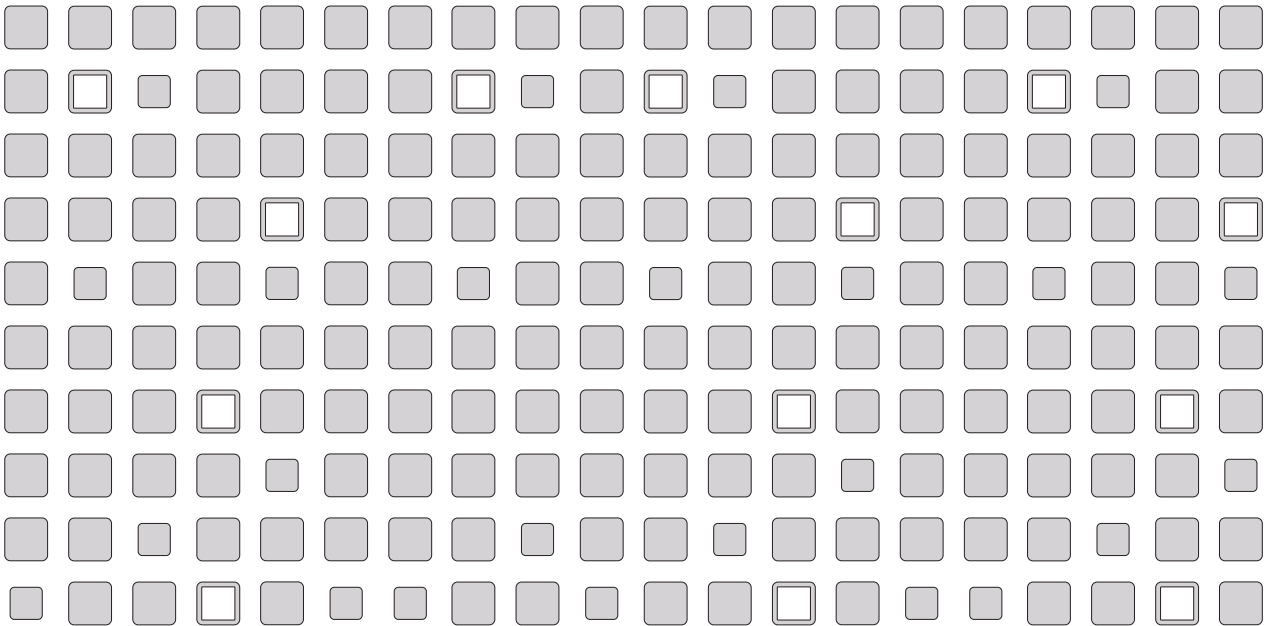


VERSION 3.0

GSX Server™ 3

Enterprise-Class Virtual Infrastructure for Intel-Based Servers

Administration Guide



VMware, Inc.

3145 Porter Drive
Palo Alto, CA 94304
www.vmware.com

Please note that you will always find the most up-to-date technical documentation on our Web site at <http://www.vmware.com/support/>.

The VMware Web site also provides the latest product updates.

Copyright © 1998–2004 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,397,242, 6,496,847, 6,704,925 and 6,711,672; patents pending. VMware is a registered trademark and the VMware boxes logo, GSX Server, ESX Server, Virtual SMP and VMotion are trademarks of VMware, Inc. Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Linux is a registered trademark of Linus Torvalds. All other marks and names mentioned herein may be trademarks of their respective companies. Revision 20040421 Version: 3.0 Item: GSX-ENG-Q104-016

Table of Contents

Introduction and System Requirements	9
VMware GSX Server: Enterprise-Class Virtual Infrastructure for Intel-Based Servers	10
Welcome to VMware GSX Server	12
Enterprise-Class Virtual Infrastructure for Intel-Based Servers	13
What's New in Version 3	14
Features in Version 3	14
Host System Requirements	19
Server Requirements	19
Remote Client Requirements	23
Virtual Machine Specifications	26
Supported Guest Operating Systems	29
Technical Support Resources	31
Documentation on the Web	31
VMware Knowledge Base	31
VMware Community Forums and Newsgroups	31
Reporting Problems	31
Log Files	32
 Installing VMware GSX Server	 37
Selecting Your Host System	38
About the VMware Virtual Machine Console on the Server	39
Installing VMware GSX Server on a Windows Host	40
Basic Installation	40
Default Directories	42
Installing the GSX Server Software on a Windows Host	43
Installing VMware GSX Server on a Linux Host	50
Basic Installation	50
Default Directories	53
Installing the GSX Server Software on a Linux Host	53
Installing the VMware Management Interface on a Linux Host	58
Installing an X Server	59
Before You Install on a SuSE Linux 7.1 or Later Host	59
Before You Install on a SuSE Linux Enterprise Server 8 Host	60

Before You Install the VMware Management Interface on a Linux Host _____	60
Configuring Web Browsers for Use with GSX Server _____	61
Launching the VMware Virtual Machine Console from the Management Interface on an Encrypted Server _____	61
Connecting to the Management Interface on a Proxy Server _____	62
Launching Help in Netscape on a Linux System _____	63
Installing the VMware Virtual Machine Console _____	64
Installing the VMware Virtual Machine Console on a Windows Host _____	64
Installing the VMware Virtual Machine Console on a Linux Host _____	67
Installing the VMware Scripting APIs _____	69
Installing the VmPerl and VmCOM Scripting APIs on a Windows Host _____	69
Installing the VmPerl API on a Linux Host _____	72
Uninstalling VMware GSX Server _____	73
Uninstalling GSX Server on a Windows Host _____	73
Uninstalling GSX Server on a Linux Host _____	78
Upgrading VMware GSX Server _____	79
Preparing for the Upgrade _____	80
Before You Install VMware GSX Server _____	80
When You Remove an Existing Version and Install the New Version _____	82
Upgrading on a Windows Host _____	83
Upgrading on a Linux Host _____	84
Using Virtual Machines Created with Version 2 under Version 3 _____	85
Creating Everything New from the Start _____	85
Using an Existing Virtual Machine without Upgrading the Virtual Hardware _____	85
Using an Existing Virtual Machine and Upgrading the Virtual Hardware _____	85
Upgrading Virtual Hardware in the Guest Operating System _____	86
Using Virtual Machines Created with Version 1 under Version 3 _____	95
Upgrading Virtual Hardware in the Guest Operating System _____	95
Managing Virtual Machines and the VMware GSX Server Host _____	99
Remotely Managing Virtual Machines _____	101
Changing the Port Number for VMware Virtual Machine Console Connections _____	101

Downloading the VMware Virtual Machine Console _____	104
Securing Virtual Machines and the Host _____	106
Understanding Permissions and Virtual Machines _____	106
Authenticating Users and Running Virtual Machines on a GSX Server for Windows Host _____	108
Authenticating Users and Running Virtual Machines on a GSX Server for Linux Host _____	111
Checking Permissions in the VMware Management Interface _____	112
Securing Your Remote Sessions _____	112
Identifying a Virtual Machine by Its UUID _____	115
Specifying a UUID for a Virtual Machine _____	116
Logging GSX Server Events on Windows _____	117
Backing Up Virtual Machines _____	119
Using a Backup Agent in the Virtual Machine _____	119
Using a Backup Agent Running on the Host Operating System _____	119
Backing Up the GSX Server Host _____	120
Considerations for Backing Up Virtual Machines _____	120
Using the VMware Management Interface _____	121
Setting the Session Length for the VMware Management Interface _____	122
Logging In to the VMware Management Interface _____	122
Using the Status Monitor _____	124
Configuring a Virtual Machine _____	130
The Apache Server and the VMware Management Interface _____	141
Logging Out of the VMware Management Interface _____	141
Deleting Virtual Machines _____	142
Deleting a Virtual Machine Using the VMware Virtual Machine Console _____	142
Deleting a Virtual Machine Using the VMware Management Interface _____	142
Configuring the GSX Server Host _____	143
Configuring GSX Server from the Management Interface _____	143
Setting User Preferences for the VMware GSX Server Host _____	149
Setting Global Preferences for VMware GSX Server _____	154
Setting a MIME Type to Launch the VMware Virtual Machine Console _____	157

Moving and Sharing Virtual Machines	161
Moving a VMware GSX Server 3 Virtual Machine	163
Virtual Machines Use Relative Paths	163
Preparing Your Virtual Machine for the Move	163
Moving a Virtual Machine to a New Host	164
Moving a GSX Server 2 Virtual Machine	166
Virtual Machines Use Relative Paths	166
Preparing Your Virtual Machine for the Move	166
Moving a Virtual Machine to a New Host	167
Moving Older Virtual Machines	169
Virtual Machines May Use Relative or Absolute Paths	169
Preparing Your Virtual Machine for the Move	169
Preparing the New Host Machine	170
Considerations for Moving Disks in Undoable Mode	171
Sharing Virtual Machines with Other Users	173
 Performance Tuning and the VMware GSX Server Host	 175
Configuring and Maintaining the Host Computer	176
Configuring GSX Server	177
General GSX Server Options	177
GSX Server on a Windows Host	181
GSX Server on a Linux Host	184
Understanding Memory Usage	185
Memory Use on the Host	185
Specifying How Much RAM is Used by All Running Virtual Machines	185
Memory Usage on Older Linux Hosts	188
 High-Availability Configurations with VMware GSX Server	 191
Using SCSI Reservation to Share SCSI Disks with Virtual Machines	192
SCSI Reservation Support	193
Enabling SCSI Reservation	194
Issues to Consider When Sharing Disks	196
Overview of Clustering with GSX Server	197
Applications That Can Use Clustering	198
Clustering Software in Virtual Machines	198
Creating a Cluster in a Box	199
Configuring Virtual Machines for Cluster in a Box	200

Creating a Two-Node Cluster with Microsoft Clustering Services on a Single GSX Server Computer _____	201
Using Network Load Balancing with GSX Server _____	208
Overview of Network Load Balancing Clusters _____	208
Creating a Multinode Network Load Balancing Cluster _____	209
Creating Two-Node Clusters Using Novell Clustering Services _____	213
Creating the First Node's Base Virtual Machine _____	213
Creating the Second Node in the Cluster _____	214
Installing the Guest Operating System and VMware Tools _____	214
Adding the Shared Disks to Both Virtual Machines _____	214
Installing Novell Clustering Services on the Cluster Nodes _____	215
Glossary _____	217
Index _____	223

1

CHAPTER

Introduction and System Requirements

This section contains the following topics introducing you to VMware GSX Server.

- [VMware GSX Server: Enterprise-Class Virtual Infrastructure for Intel-Based Servers on page 12](#)
- [Welcome to VMware GSX Server on page 14](#)
- [What's New in Version 3 on page 16](#)
- [Host System Requirements on page 21](#)
- [Virtual Machine Specifications on page 28](#)
- [Supported Guest Operating Systems on page 31](#)
- [Technical Support Resources on page 33](#)

VMware GSX Server: Enterprise-Class Virtual Infrastructure for Intel-Based Servers

VMware® GSX Server™ is virtual infrastructure for enterprise IT administrators who want to consolidate servers and streamline development and testing operations. GSX Server is easily installed and managed, and provides rapid return on investment (ROI). Unlike other virtualization products, GSX Server is enterprise-proven, preserves freedom of choice and offers an upgrade path to datacenter-class virtualization.

With over three years of proven success, thousands of customers trust VMware GSX Server as their virtualization solution. Easily installed on Windows or Linux platforms, GSX Server provides advanced capabilities that make it the most flexible server virtualization product on the market. GSX Server is part of the widely deployed VMware virtual infrastructure solution with virtual machines compatible across all VMware products, and with unified management and provisioning provided by VMware VirtualCenter.

VMware GSX Server simplifies computing infrastructure by partitioning and isolating servers in secure and transportable virtual machines, each of which can run standard Windows, Linux or NetWare operating systems and applications. GSX Server allows you to remotely manage, automatically provision and standardize virtual machines on a secure, uniform platform.

Thousands of enterprise customers rely on VMware GSX Server to deliver server scalability, reliability and high availability and to maximize return on IT investments. Use GSX Server across the enterprise to:

- Streamline software development and testing operations with easily provisioned and managed server-based virtual machines.
- Implement server consolidation for new and legacy departmental server applications.
- Provision servers rapidly to local or remote locations.
- Streamline operating system and application patch management.

Key GSX Server 3 Benefits

GSX Server 3 offers the following key benefits:

- Shipping for over three years with thousands of successful customers, VMware GSX Server is the most flexible and easily deployed server virtualization product on the market.
- Offers widest selection of supported host and guest operating systems of any virtualization technology — preserves your freedom to choose the best operating system platform.
- Integrates easily into any environment for ultimate versatility — installs like an application and runs on any standard x86 hardware.
- Supports large server — up to 64GB of host memory, 32 host processors and 64 powered-on virtual machines — for ultimate scalability, extensibility and robustness.
- Offers virtual machine compatibility across the entire VMware family of virtualization products and is ready to run with VMware VirtualCenter.
- Supports advanced virtual machine clustering for high-availability applications.
- Ensures reliable server consolidation through isolated virtual partitions.
- Allows secure remote management.
- Permits full network connectivity for virtual machines.
- Automates monitoring and control of virtual machines with VmCOM and VmPerl Scripting APIs.
- Runs virtual disk files on any system with current VMware software installed.

To discover more new features of VMware GSX Server 3, see [What's New in Version 3 on page 16](#).

Welcome to VMware GSX Server

Thank you for choosing VMware GSX Server, the software that provides IT professionals with enterprise-class server consolidation and high availability of server resources by letting them run multiple operating systems in secure, transportable, high-performance virtual computers.

If you're new to GSX Server, this chapter is the place to start.

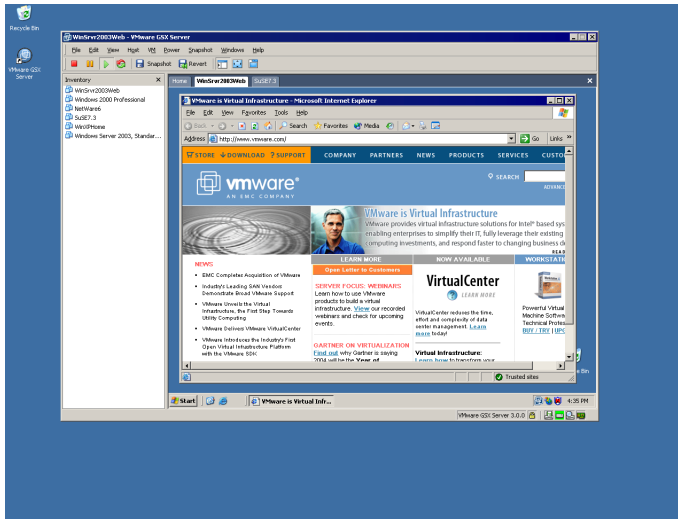
If you're a veteran user of VMware products, take a few minutes to see what's new in version 3 and check out the notes on upgrading your installation.

The *VMware GSX Server Administration Guide* introduces you to some of the things you can do with GSX Server and guides you through the key steps for installing the software, configuring your server host and managing your virtual machines.

The *VMware GSX Server Virtual Machine Guide* provides information on creating virtual machines, as well as in-depth reference material for getting the most out of the sophisticated features of GSX Server.

Enterprise-Class Virtual Infrastructure for Intel-Based Servers

VMware products provide a virtualization layer that turns your physical computers into a pool of logical computing resources. You can then dynamically allocate those resources to any operating system or application in the way that best meets your needs. You'll be able to spend more time delivering tangible value to your business and less time installing operating systems, rebooting and reconfiguring hardware.



Run the operating systems you need — all at once.

With VMware virtualization technology, you can set up completely independent installations of operating systems on a single machine. Multiple instances of Microsoft® Windows® or Linux® can run side by side in virtual machines that you create with the GSX Server software. Each virtual machine is equivalent to a server with a unique network address and a full complement of hardware devices. You install and run a complete, unmodified operating system and application software, just as you do on a physical server.

Host and Guest

- The physical computer on which you install the GSX Server software is called the host computer, and its operating system is called the host operating system.
- The operating system running inside a virtual machine is called a guest operating system.
- For definitions of these and other special terms, see the glossary at the end of this manual.

What's New in Version 3

Whether you're a long-time power user of VMware GSX Server or a new user who is just learning what you can do with virtual machines, the new features in VMware GSX Server 3 extend its capabilities and make it easier to use.

Features in Version 3

Here are some highlights of key features to explore in VMware GSX Server 3:

GSX Server 3 Security Update: OpenSSL 0.9.7d Patches

Patches are available for GSX Server 3 that update the version of OpenSSL used in the product. The new version of OpenSSL corrects security vulnerabilities and is posted on the GSX Server Security Updates page at www.vmware.com/download/gsx_security.html.

GSX Server 3 users are strongly urged to download and install these patches.

Enhanced Virtual Machine User Access Control

On Windows hosts, a virtual machine runs as a user. You can specify the particular user or let the virtual machine run as the user that powers it on. For more information, see [Authenticating Users and Running Virtual Machines on a GSX Server for Windows Host on page 108](#).

Improved Security for Remote Connections

SSL is enabled by default for remote connections with the VMware Virtual Machine Console and the VMware Management Interface.

VirtualCenter Ready

GSX Server 3 is enabled for management by an upcoming release of VMware VirtualCenter. You will be able to use VirtualCenter to manage and provision virtual machines on multiple GSX Server hosts, then migrate the virtual machines between other GSX Server and ESX Server systems under VirtualCenter management.

New VMware Virtual Machine Console

Connect to and manage virtual machines with the VMware Virtual Machine Console, which combines the best abilities of the local and remote consoles in one application. Create and configure virtual machines locally and remotely. Connect to virtual machines from the local server or remote client at the same time, while other consoles are already connected. Run virtual machines in full screen mode locally and remotely.

The console interface is completely updated. You can run multiple virtual machines in the same window and switch from one to another using the new quick switch mode. The console menus have been streamlined. The console requires less network bandwidth over remote connections than the older console did.

For details, see [Running Virtual Machines](#) in the *VMware GSX Server Virtual Machine Guide*.

Take Snapshots of Your Virtual Machines

You can take a snapshot of your virtual machine's state, a point-in-time copy of the running system state, that is saved to disk. You can revert to that snapshot at any time — making it easier to do challenging tasks like upgrading guest operating systems. Take a snapshot, upgrade the operating system, and if something goes wrong, revert back to the snapshot. Or use the snapshot as a starting point for a sales demonstration.

See [Taking Snapshots](#) in the *VMware GSX Server Virtual Machine Guide* for details.

Automatically Install GSX Server on Windows Hosts and VMware Tools in Windows Guests

We've improved the installers for Windows hosts and for VMware Tools in Windows guest operating systems. GSX Server for Windows hosts and VMware Tools for Windows guests use the Microsoft Windows Installer runtime engine, which allows you to automate the installation of GSX Server on a Windows host and VMware Tools in a Windows virtual machine. For information, see [Automating the Installation of GSX Server on page 47](#) and [Automating the Installation of VMware Tools in a Windows Guest](#) in the *VMware GSX Server Virtual Machine Guide*.

With the Microsoft Windows Installer runtime engine, you can pick and choose the features you want to install.

Automatically Start and Stop Virtual Machines When the Host Starts and Stops

You can configure virtual machines to automatically power on when the GSX Server host starts or automatically power off when the GSX Server host shuts down. For more information, see [Powering Virtual Machines On and Off when the Host Starts and Shuts Down](#) in the *VMware GSX Server Virtual Machine Guide*.

Connect to Older Virtual Machines and Older GSX Server Hosts

You can connect to older GSX Server hosts with consoles and run virtual machines from older versions of VMware products. For information, see [Connecting to Older GSX Server and ESX Server Systems and Older Virtual Machines](#) in the *VMware GSX Server Virtual Machine Guide*.

Improved VMware Management Interface

Managing virtual machines and the GSX Server host from a Web browser just got better. You can configure more host and virtual machine features, including virtual machine hardware, configuration options and SSL connections. For more information, see [Using the VMware Management Interface on page 121](#).

Log GSX Server Events on Windows Hosts

GSX Server sends information about certain events that occur in the application on Windows hosts to the Windows Event Viewer. For details, see [Logging GSX Server Events on Windows on page 117](#).

Improved Virtual Disk and Networking Performance

Experience 10 to 20% improvement in virtual disk and networking performance.

Monitor Virtual Machine Performance on Windows Hosts

Use GSX Server specific counters with the Windows Performance console (PerfMon) to monitor the performance of running virtual machines on Windows hosts. For details, see [Monitoring Virtual Machine Performance on page 181](#).

More Memory for Your Virtual Machines

Allocate up to 3600MB of memory to each virtual machine to run large server applications. For more information, see [Allocating Memory to a Virtual Machine](#) in the *VMware GSX Server Virtual Machine Guide*.

Easier Sharing of Virtual Machines with Latest VMware Products

Virtual machines created with GSX Server 3 are compatible with VMware Workstation 4 and ESX Server 2 for easier migrating and sharing of virtual machines.

New LSI Logic Virtual SCSI Adapter for Guest Operating Systems

The LSI Logic virtual SCSI adapter is included when you install Windows Server 2003, Red Hat Enterprise Linux 3.0 or NetWare guests.

PXE Boot

Boot virtual machines over your network and install guest operating systems from a PXE server. For more information, see [Using PXE with Virtual Machines](#) in the *VMware GSX Server Virtual Machine Guide*.

Easier Virtual Networking Configuration

On Windows hosts, use the Virtual Network Editor to configure virtual networking easily. For more information, see [Networking](#) in the *VMware GSX Server Virtual Machine Guide*.

Network Adapter Teaming Support

On Windows hosts, virtual machines can bridge to teamed or bonded host network adapters. For more information, see [Configuring Bridged Networking when Using Teamed Network Interface Cards on Your Host](#) in the *VMware GSX Server Virtual Machine Guide*.

Generic SCSI Tape Backup Support

Back up virtual machines using popular backup software and SCSI tape devices. For more information, see [Backing Up Virtual Machines on page 119](#).

Using DVD-ROM and CD-ROM Drives on Remote Clients

If you're connected to a virtual machine remotely from a client, you can use the local DVD-ROM or CD-ROM drive to install software or copy data without needing to use the drive on the GSX Server host. For more information, see [Using the DVD-ROM or CD-ROM Drive on a Client](#) in the *VMware GSX Server Virtual Machine Guide*.

Improved Virtual DVD-ROM and CD-ROM Drive Support

Read multisession DVD-ROM and CD-ROM media. Burn CD-ROMs in your guest operating systems.

Debugging Support in Virtual Machines

GSX Server supports user- and kernel-level debuggers in virtual machines.

New Operating System Support

Get the freedom to choose the operating systems and applications that work best for you. VMware GSX Server 3 provides support for Red Hat™ Enterprise Linux 3.0, SuSE Linux Enterprise Server 8.0 patch 3 and Turbolinux Server 8.0 and Workstation 8.0 hosts. New supported guest operating systems include Red Hat Enterprise Linux 3.0; SuSE Linux Enterprise Server 7 patch 2; NetWare 6.5 Server; FreeBSD 4.6.2, 4.8, 5.0 and 5.1 (prerelease version); and Turbolinux Server 7.0, 8.0 and Workstation 8.0. Experimental support for Microsoft Windows code-named Longhorn is provided.

New Linux Kernel Support

Run your Linux guest operating systems with the new 2.6 kernel.

New Support Scripts

When you file support requests, please use the new support scripts to collect data that help us diagnose your problems. For details, see [Reporting Problems on page 33](#).

Automatically Check for Product Updates

VMware GSX Server now checks automatically to see if updates for the product are available. You can specify what interval to use for the automatic check or switch to

manual checks only. For more information, see [Updating GSX Server Software Automatically on page 150](#).

Host System Requirements

What do you need to get the most out of VMware GSX Server? Take the following list of requirements as a starting point. Remember that the virtual machines running under GSX Server are like physical computers in many ways — and, like physical computers, they generally perform better if they have faster processors, more memory and sufficient disk space.

Be aware that system requirements may change after this manual has been printed. For the latest system requirements, go to the VMware Web site at www.vmware.com/support/gsx3/doc/intro_sysreqs_host_gsx.html.

Note: VMware GSX Server 3 is supported only on host processors and host operating systems running in 32-bit mode; operating systems and Intel processors running in 64-bit mode are not supported.

Note: VMware GSX Server (for Windows and Linux hosts) is not localized and does not support internationalization. However, virtual machines created with the localized version of VMware Workstation for Windows still work with GSX Server, even though certain elements do not display properly in GSX Server.

Server Requirements

Server Host Hardware

VMware GSX Server supports up to 32-way multiprocessor servers. The number of virtual machines you can run concurrently depends on the resources they require, but VMware recommends you run no more than four virtual machines concurrently per processor. You can run a maximum of 64 virtual machines concurrently on one host. The server must include the following.

- Standard x86-based server with up to 32 CPUs
- 733MHz or faster compatible x86 processor that supports the Pentium® instruction set

Compatible processors include

- Intel®: Pentium II, Pentium III, Pentium III Xeon, Pentium 4, Xeon
- AMD™: Athlon™, Athlon XP

Multiprocessor systems supported

Memory

You need enough memory to run the Windows or Linux host operating system, plus memory required for each guest operating system and applications on the host and

each guest; see your guest operating system and application documentation for their memory requirements.

- Minimum: 512MB
- Maximum: 64GB for Windows hosts and Linux hosts that support large memory or are PAE-enabled, 4GB for non-PAE-enabled Windows hosts or 2GB for Linux hosts with kernels in the 2.2.x series

Display

- 16-bit display adapter recommended; greater than 256-color (8-bit) display adapter required

Note: Linux hosts must have an X server that meets the X11R6 specification (such as XFree86) and a video adapter supported by that server to run guest operating systems in full screen mode. If an X server is not installed, you must install one, such as XFree86. XFree86 version 3.3.4 or higher is recommended, with XFree86 4.0 preferred.

Host Hard Disk

- 130MB free disk space on Windows hosts required for server, VMware Management Interface, VmPerl API, VmCOM API and VMware Virtual Machine Console installation
- 20MB free disk space on Linux hosts required for server, VMware Management Interface, VmPerl API and VMware Virtual Machine Console installation
- At least 1GB free disk space recommended for each guest operating system and the application software used with it; using a default setup, the actual disk space needs are approximately the same as those for installing and running the guest operating system and applications on a physical computer
- IDE or SCSI hard drives, CD-ROM and DVD-ROM drives supported
- Guest operating systems can reside in virtual disk files or on physical (raw) disk partitions

Local Area Networking

- Any Ethernet controller that the host operating system supports
- Non-Ethernet networks are supported using built-in network address translation (NAT) or using a combination of host-only networking plus routing software on the host operating system
- A static IP address for your host machine (recommended)

Windows Host Operating Systems

You need a Windows **server** operating system. If you intend to use the VMware Management Interface, Internet Information Server (IIS) 5.0 or 6.0 must be installed.

- Windows Server 2003 Enterprise Edition
- Windows Server 2003 Standard Edition
- Windows Server 2003 Web Edition
- Microsoft Windows 2000 Advanced Server, Service Pack 3 and Service Pack 4
- Microsoft Windows 2000 Server, Service Pack 3 and Service Pack 4

The VmPerl API requires Perl 5.005x or higher.

The VMware Management Interface requires one of these browsers:

- Internet Explorer 5.5 or 6.0 (6.0 highly recommended)
- Netscape® Navigator 7.0
- Mozilla 1.x

Note: As new browser versions are released, VMware tests the management interface for stability and reliability with these versions. We make every effort to add support for new browser versions in a timely manner, but until a browser is added to the above list, its use with our product is not supported. For the latest system requirements, go to the VMware Web site at www.vmware.com/support/gsx3/doc/intro_sysreqs_host_gsx.html.

Linux Host Operating Systems

Supported distributions and kernels are listed below. GSX Server may not run on systems that do not meet these requirements.

- Mandrake Linux 9.2
- Mandrake Linux 9.0
- Mandrake Linux 8.2
- Red Hat Enterprise Linux 3.0 AS
- Red Hat Enterprise Linux 3.0 ES
- Red Hat Enterprise Linux 3.0 WS
- Red Hat Enterprise Linux AS 2.1
- Red Hat Enterprise Linux ES 2.1
- Red Hat Enterprise Linux WS 2.1
- Red Hat Linux 9.0

- Red Hat Linux 8.0
- Red Hat Linux 7.3
- Red Hat Linux 7.2
- Red Hat Linux 7.1
- SuSE™ Linux Enterprise Server 8
- SuSE Linux Enterprise Server 7
- SuSE Linux 9.0
- SuSE Linux 8.2
- SuSE Linux 8.1
- SuSE Linux 8.0
- SuSE Linux 7.3
- Turbolinux Server 8.0
- Turbolinux Workstation 8.0
- Turbolinux Server 7.0

Platforms not listed above are not supported.

Note: As new Linux kernels and distributions are released, VMware modifies and tests its products for stability and reliability on those host platforms. We make every effort to add support for new kernels and distributions in a timely manner, but until a kernel or distribution is added to the list below, its use with our product is not supported. Look for newer prebuilt modules in the Download area of our Web site. Go to www.vmware.com/download/. For the list of supported kernels, go to the VMware Web site at www.vmware.com/support/gsx3/doc/intro_sysreqs_host_gsx.html.

Other Linux host operating system requirements include:

- Linux kernel 2.2.14-5.0 is not supported
- Standard Linux **server** installation is required with `glibc` version 2.1 or higher and `libcXpm.so`
- The `inetd` process, which must be configured and active for VMware Virtual Machine Console and VMware Management Interface connections
- Version 2.1.36 of the SCSI Generic (`sg.o`) driver is required to use generic SCSI devices in virtual machines
- Perl 5.005x or higher is required to use VmPerl API
- X server is required to run the VMware Virtual Machine Console

In addition, the VMware Management Interface requires one of these browsers:

- Netscape® Navigator 7.0
- Mozilla 1.x

Note: As new browser versions are released, VMware tests the management interface for stability and reliability with these versions. We make every effort to add support for new browser versions in a timely manner, but until a browser is added to the above list, its use with our product is not supported. For the latest system requirements, go to the VMware Web site at

www.vmware.com/support/gsx3/doc/intro_sysreqs_host_gsx.html.

Information about Running GSX Server on Some SuSE Linux Hosts

Keep in mind the following when you run GSX Server on these SuSE Linux hosts.

- **SLES 8** — Install `gcc` on your SLES 8 host before installing GSX Server.
- **SLES 7** — If you intend to upgrade the kernel, make sure you deselect any Samba components when you apply the update patch, as the patch incorrectly updates Samba on your host. Running the update with the Samba packages selected can result in serious issues on your host like system hangs or segmentation faults.

VmPerl and VmCOM Scripting APIs

The VmPerl API includes the `vmware-cmd` utility. The VmCOM API works on Windows Server 2003 and Windows 2000 hosts only. For more information, go to the VMware Web site at www.vmware.com/support/developer.

Remote Client Requirements

The remote client is a Windows or Linux system from which you launch the VMware Virtual Machine Console or use VMware Scripting APIs to remotely manage virtual machines on the GSX Server host. You access the VMware Management Interface to manage virtual machines on the host using a Web browser.

Hardware Requirements

- Standard x86-based computer
- 266MHz or faster processor
- 64MB RAM minimum
- 20MB (for Windows hosts) or 10MB (for Linux hosts) free disk space is required for installation of the VMware Virtual Machine Console

- 17MB free disk space is required for VMware Scripting APIs (VmCOM and VmPerl Scripting APIs) installation on Windows remote clients; 14MB is required for VmPerl API on Linux remote clients

Software - Windows Remote Client

- Windows Server 2003 Standard edition, Windows Server 2003 Enterprise edition and Windows Server 2003 Web edition
- Windows XP Professional and Windows XP Home Edition Service Pack 1
- Windows 2000 Professional, Server and Advanced Server, Service Pack 1, Service Pack 2, Service Pack 3 and Service Pack 4
- Windows NT 4.0 Workstation and Server, Service Pack 6a
- The VMware Management Interface requires one of these browsers:
 - Internet Explorer 5.5 or 6.0 (6.0 highly recommended)
 - Netscape Navigator 7.0
 - Mozilla 1.x

Note: As new browser versions are released, VMware tests the management interface for stability and reliability with these versions. We make every effort to add support for new browser versions in a timely manner, but until a browser is added to the above list, its use with our product is not supported. For the latest system requirements, go to the VMware Web site at

www.vmware.com/support/gsx3/doc/intro_sysreqs_host_gsx.html.

Software - Linux Remote Client

- Standard Linux installation is required with glibc version 2.1 or higher and one of the following kernels:
 - For single-processor systems: kernel 2.0.32 or higher in the 2.0.x series, or kernel in the 2.2.x series or 2.4.x series
 - For SMP systems: kernel in the 2.2.x series or 2.4.x series

Note: Linux kernel 2.2.14-5.0 is not supported.

- Perl 5.005x or higher is required to use VmPerl API
- X server is required to run the VMware Virtual Machine Console on the client
- The VMware Management Interface requires one of these browsers:
 - Netscape Navigator 7.0
 - Mozilla 1.x

Note: As new browser versions are released, VMware tests the management interface for stability and reliability with these versions. We make every effort to add support for new browser versions in a timely manner, but until a browser is added to the above list, its use with our product is not supported. For the latest system requirements, go to the VMware Web site at www.vmware.com/support/gsx3/doc/intro_sysreqs_host_gsx.html.

VmPerl and VmCOM Scripting APIs

The VmPerl API includes the `vmware-cmd` utility. The VmCOM API works on Windows Server 2003, Windows XP, Windows 2000 and Windows NT clients only. For more information, go to the VMware Web site at www.vmware.com/support/developer.

Virtual Machine Specifications

Each virtual machine created with GSX Server provides a platform that includes the following devices that your guest operating system can see.

Virtual Processor

- Same processor as that on host computer
- Single processor per virtual machine on symmetric multiprocessor (SMP) systems

Virtual Chip Set

- Intel 440BX-based motherboard with NS338 SIO chip and 82093AA IOAPIC

Virtual BIOS

- PhoenixBIOS™ 4.0 Release 6 with VESA BIOS
- DMI/SMBIOS-compliant for system management agent support

Virtual Memory

- Up to 3600MB of memory per virtual machine, depending upon the host system's configuration, the types of applications running on the host and the amount of memory on the host.

Virtual Graphics

- VGA and SVGA support

Virtual IDE Drives

- Up to four devices — disks, CD-ROM or DVD-ROM (DVD drives can be used to read data DVD-ROM discs; DVD video is not supported)
- Hard disks can be virtual disks or physical disks
- IDE virtual disks up to 128GB
- CD-ROM can be a physical device or an ISO image file

Virtual SCSI Devices

- Up to 21 devices on three virtual SCSI controllers
- SCSI virtual disks up to 256GB
- Hard disks can be virtual disks or physical disks
- Generic SCSI support allows scanners, CD-ROM, DVD-ROM, tape drives and other SCSI devices to be used without needing drivers in the host operating system
- Mylex® (BusLogic) BT-958 compatible host bus adapter

- LSI Logic Ultra160 LSI53C10xx SCSI controller

Virtual PCI Slots

- Six virtual PCI slots, to be divided among the virtual SCSI controllers, virtual Ethernet cards, virtual display adapter and virtual sound adapter

Virtual Floppy Drives

- Up to two 1.44MB floppy devices
- Physical drives or floppy image files

Virtual Serial (COM) Ports

- Up to four serial (COM) ports
- Output to serial ports, Windows files, Linux files or named pipes

Virtual Parallel (LPT) Ports

- Up to two bidirectional parallel (LPT) ports
- Output to parallel ports or host operating system files

Virtual USB ports

- Two-port USB 1.1 UHCI controller
- Supported devices include USB printers, scanners, PDAs, hard disk drives, memory card readers and still digital cameras

Virtual Keyboard

- 104-key Windows 95/98 enhanced

Virtual Mouse and Drawing Tablets

- PS/2 mouse
- Serial tablets supported

Virtual Ethernet Card

- Up to four virtual Ethernet cards
- AMD PCnet-PCI II compatible
- Wireless networking supported with bridged and NAT networking
- PXE ROM version 2.0

Virtual Networking

- Nine virtual Ethernet switches (three configured by default for bridged, host-only and NAT networking)

- Virtual networking supports most Ethernet-based protocols, including TCP/IP, NetBEUI, Microsoft Networking, Samba, Novell® NetWare® and Network File System
- Built-in NAT supports client software using TCP/IP, FTP, DNS, HTTP and Telnet

Virtual Sound Adapter

- Sound output and input
- Creative Labs Sound Blaster® AudioPCI emulated (MIDI input, game controllers and joysticks not supported)

Supported Guest Operating Systems

The operating systems listed here have been tested in VMware GSX Server 3 virtual machines and are officially supported. For notes on installing the most common guest operating systems, see the *VMware Guest Operating System Installation Guide*, available from the VMware Web site or from the Help menu.

Operating systems that are not listed are not supported for use in a VMware GSX Server virtual machine. For the most recent list of supported guest operating systems, visit the VMware Web site at

www.vmware.com/support/gsx3/doc/intro_sysreqs_guest_gsx.html.

Microsoft Windows

- Microsoft Windows code named Longhorn (experimental support)
- Windows Server 2003 Web Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition and Windows Small Business Server 2003
- Windows XP Professional and Windows XP Home Edition, including Service Pack 1 and Service Pack 2 Beta
- Windows 2000 Professional, Windows 2000 Server and Windows 2000 Advanced Server, including Service Pack 1, Service Pack 2, Service Pack 3 and Service Pack 4 and Windows 2000 Professional Service Pack 4 checked build
- Windows NT® 4.0 Server Service Pack 6a, Windows NT Workstation 4.0, including Service Pack 6a and Windows NT 4.0 Terminal Server Edition Service Pack 6a
- Windows Me
- Windows 98 (including latest Customer Service Packs) and Windows 98 SE
- Windows 95 (including Service Pack 1 and all OSR releases)
- Windows for Workgroups 3.11
- Windows 3.1

Microsoft MS-DOS

- MS-DOS 6.22

Linux

- Mandrake Linux 8.0, 8.1, 8.2, 9.0, 9.1 and 9.2
- Red Hat Linux 6.2, 7.0, 7.1, 7.2, 7.3, 8.0 and 9.0, Red Hat Enterprise Linux (AS, ES, WS) 2.1 and Red Hat Enterprise Linux (AS, ES, WS) 3.0

- SuSE Linux 7.3, 8.0, 8.1, 8.2 and 9.0, SuSE Linux Enterprise Server 7 (including patch 2) and 8 (including patch 3)
- Turbolinux Server 7.0, 8.0, Workstation 8.0

Novell NetWare

- NetWare 4.2 Support Pack 9, 5.1 Support Pack 6, 6.0 Support Pack 3 and 6.5 Support Pack 1

FreeBSD

- FreeBSD 4.0–4.6.2, 4.8 and 5.0

Technical Support Resources

Documentation on the Web

Full documentation for VMware GSX Server, including the latest updates to the manual, can be found on the VMware Web site at www.vmware.com/support/gsx3/doc.

VMware Knowledge Base

You can find troubleshooting notes and tips for advanced users in the knowledge base on the VMware Web site at www.vmware.com/support/kb/enduser/std_alp.php.

VMware Community Forums and Newsgroups

The VMware community is a set of moderated discussion forums hosted on the VMware Web site and is open to users of all VMware products. VMware technical staff regularly monitor the forums to learn about your issues and feedback, and help facilitate discussions when appropriate.

To participate in the community, go to www.vmware.com/community and create a user account.

The VMware newsgroups are primarily forums for users to help each other. You are encouraged to read and post issues, work-arounds and fixes. While VMware personnel may read and post to the newsgroups, they are not a channel for official support. The VMware NNTP news server is at news.vmware.com.

For a listing of all current newsgroups and the topic areas they cover, see www.vmware.com/support/newsgroups.html.

Reporting Problems

If you have problems while running GSX Server, please report them to the VMware support team.

You must register your serial number; then you can report your problems by submitting a support request at www.vmware.com/requestsupport.

These guidelines describe the information we need from you to diagnose problems. This information largely comes from various log files. Which log file we need depends upon the problem you encounter. The log files are listed below.

You can simplify the process of collecting the needed information by running the support script to collect the appropriate log files and system information. Follow the steps below that apply to your host computer.

Note: The support script runs only on the GSX Server host. If you encounter problems on a remote client, you must supply the log files manually. The two log files you should supply, depending upon the problem you encounter on the client, include the VMware Virtual Machine Console log file and the installation log file. See below for more information about these logs.

Windows Host

1. Open a command prompt.
2. Change to the GSX Server program directory.

```
C:
cd \Program Files\VMware\VMware GSX Server
```

If you did not install the program in the default directory, use the appropriate drive letter and substitute the appropriate path in the `cd` command above.
3. Run the support script.

```
cscript vm-support.vbs
```
4. After the script runs, it displays the name of the directory where it has stored its output. Use a file compression utility such as WinZip or PKZIP to zip that directory, then include the zip file with your support request.

Linux Host

1. Open a terminal.
2. Run the support script as the user who is running the virtual machine or as root.

```
vm-support
```

If you are not running the script as root, the script displays messages indicating that it cannot collect some information. This is normal. If the VMware support team needs that information, a support representative may ask you to run the script again as root.
3. The script creates a compressed `.tgz` file in the current directory. Include that output file with your support request.

Log Files

The following log files are generated by GSX Server and are collected by the support script as needed. Since there is no support script on a remote client, you need to submit a support request at www.vmware.com/requestsupport for any issues you encounter on a client and include the console's log file or its installation log file.

Virtual Machine Log File

If a virtual machine exits abnormally or crashes, please run the support script or save the log file before you launch that virtual machine again. The key log file to save is the VMware log file for the affected virtual machine.

On a Windows host, the `vmware.log` file is in the same directory as the configuration file (`.vmx`) of the virtual machine that had problems. The path to the log file of the active virtual machine appears in the About dialog box. In a console, choose **Help > About VMware GSX Server**, and look under **Additional information**.

On a Linux host, the `<vmname>.log` file is in the same directory as the configuration file (`.vmx`) of the virtual machine that had problems.

Also save any core files (`core` or `vmware-core`).

Virtual Machine Event Log File

The virtual machine's event log, some of which can be viewed in the VMware Management Interface, is stored as a file on the host. This file can also be useful in the event a virtual machine crashes.

Each virtual machine on the host includes an event log file called `event-<path_to_configuration_file>.vmx.log`.

On a Windows host, the log is stored in `C:\Program Files\VMware\VMware GSX Server\vmserverdRoot\eventlog`.

On a Linux host, the log is stored in `/var/log/vmware`.

VMware Virtual Machine Console Log File

The VMware Virtual Machine Console keeps a log. If you encounter problems with the VMware Virtual Machine Console on a remote client, please submit a support request and this log file.

On a Windows host, the log is called `vmware-<username>-<PID>.log` and is stored in the user's TEMP directory; by default, this directory is `C:\Documents and Settings\<username>\Local Settings\Temp`. The path to this file appears in the About dialog box. In a console, choose **Help > About VMware GSX Server**, and look under **Additional information**.

On a Linux host, the log is called `ui-<PID>.log` and is stored in the user's TEMP directory; by default, this directory is `/tmp/vmware-<username>`. The path to this file appears in the terminal when you start the console.

VMware Management Interface Log File

The VMware Management Interface keeps a log.

On a Windows host, the log is called `mui.log` and is stored by default in `C:\Program Files\VMware\VMware Management Interface`.

On a Linux host, the log is called `error_log` and is stored by default in `/var/log/vmware-mui`.

VMware Authorization Service Log File

You can enable logging for the VMware Authorization Service (known as `vmware-authd` on Linux hosts) manually.

1. In a text editor, open the following file:
 - On a Windows host, edit `config.ini`, located in `C:\Documents and Settings\All Users\Application Data\VMware\VMware GSX Server`.
 - On a Linux host, edit `/etc/vmware/config`.
2. Add the following lines to the file:


```
vmauthd.logEnabled = TRUE
log.vmauthdFileName = "vmauthd.log"
```

This creates a file called `vmauthd.log`. On a Windows host, this file appears by default in `C:\Windows\system32` or `C:\WINNT\system32`; on a Linux host, this file appears by default in `/var/log/vmware`.
3. Save and close the configuration file. The log is enabled on a Linux host.
4. On a Windows host, restart the VMware Authorization Service. Choose **Start > Administrative Tools > Services**. Right-click **VMware Authorization Service** and choose **Restart**. This enables logging.

VMware Registration Service Log File

The VMware Registration Service keeps a log.

On a Windows host, the log is called `vmware-serverd.log` and is stored in `C:\Windows\Temp`.

On a Linux host, the log is called `vmware-serverd.log` and is stored in `/var/log/vmware`.

VMware GSX Server and VMware Virtual Machine Console Installation Log Files

GSX Server keeps an installation log file on the server host.

On a remote client, the VMware Virtual Machine Console keeps an installation log file. If you encounter problems installing the VMware Virtual Machine Console, please submit a support request and this log file.

On a Windows host, the file is `VMInst.log`. It is saved in your TEMP directory; the default location is `C:\Documents and Settings\<username>\Local Settings\Temp`. The `Local Settings` folder is hidden by default. To see its contents, open **My Computer**, choose **Tools > Folder Options**, click the **View** tab and select **Show Hidden Files and Folders**.

On a Linux host, the log is called `locations` and is stored in `/etc/vmware`.

Installing VMware GSX Server

The following sections describe how to install VMware GSX Server on your Linux or Windows host system:

- [Selecting Your Host System on page 38](#)
- [About the VMware Virtual Machine Console on the Server on page 39](#)
- [Installing VMware GSX Server on a Windows Host on page 40](#)
 - [Basic Installation on page 40](#)
 - [Default Directories on page 42](#)
 - [Installing the GSX Server Software on a Windows Host on page 43](#)
- [Installing VMware GSX Server on a Linux Host on page 50](#)
 - [Basic Installation on page 50](#)
 - [Default Directories on page 53](#)
 - [Installing the GSX Server Software on a Linux Host on page 53](#)
 - [Installing the VMware Management Interface on a Linux Host on page 58](#)
 - [Installing an X Server on page 59](#)

- [Before You Install on a SuSE Linux 7.1 or Later Host on page 59](#)
- [Before You Install on a SuSE Linux Enterprise Server 8 Host on page 60](#)
- [Before You Install the VMware Management Interface on a Linux Host on page 60](#)
- [Configuring Web Browsers for Use with GSX Server on page 61](#)
 - [Launching the VMware Virtual Machine Console from the Management Interface on an Encrypted Server on page 61](#)
 - [Connecting to the Management Interface on a Proxy Server on page 62](#)
 - [Launching Help in Netscape on a Linux System on page 63](#)
- [Installing the VMware Virtual Machine Console on page 64](#)
 - [Installing the VMware Virtual Machine Console on a Windows Host on page 64](#)
 - [Installing the VMware Virtual Machine Console on a Linux Host on page 67](#)
- [Installing the VMware Scripting APIs on page 69](#)
 - [Installing the VmPerl and VmCOM Scripting APIs on a Windows Host on page 69](#)
 - [Installing the VmPerl API on a Linux Host on page 72](#)
- [Uninstalling VMware GSX Server on page 73](#)
 - [Uninstalling GSX Server on a Windows Host on page 73](#)
 - [Uninstalling GSX Server on a Linux Host on page 78](#)

Selecting Your Host System

VMware GSX Server is available for both Windows and Linux host computers. The installation files for both host platforms are included on the same CD-ROM.

Your serial number allows you to use VMware GSX Server only on the host operating system for which you licensed the software. If you have a serial number for a Windows host, you cannot run the software on a Linux host, and vice versa.

To use VMware GSX Server on a different host operating system — for example, to use it on a Linux host if you have licensed the software for a Windows host — purchase a license on the VMware Web site. You may also get an evaluation license at no charge for a 15-day evaluation of the software. For more information, see www.vmware.com/download/.

To install on a supported Windows host computer, see [Installing VMware GSX Server on a Windows Host on page 40](#). To install on a Linux host computer, see [Installing VMware GSX Server on a Linux Host on page 50](#).

To review the list of supported host operating systems on which you can install GSX Server, see [Host System Requirements on page 19](#).

Upgrading from Previous Versions

If you are upgrading from a previous version of VMware GSX Server, read [Upgrading VMware GSX Server on page 79](#) before you begin.

About the VMware Virtual Machine Console on the Server

VMware GSX Server now uses a single console — the VMware Virtual Machine Console — to manage virtual machines on any GSX Server host directly from the host or remotely from a client workstation or another host.

Previous versions had separate local and remote consoles that provided different levels of control over virtual machines and different levels of performance.

Multiple consoles can connect to a virtual machine at the same time, giving multiple authorized users concurrent access to the virtual machine; similarly, multiple users can connect to the virtual machine with VMware Scripting APIs and the VMware Management Interface. You can run virtual machines in full screen mode from any console.

When you install the GSX Server software, the VMware Virtual Machine Console is installed automatically. You should install the console on any client workstation from which you want to access virtual machines. This allows for remote management of virtual machines.

To install the console on a client, see [Installing the VMware Virtual Machine Console on page 64](#). You can download the console from the VMware Management Interface for convenient installation on a remote client. For more information, see [Downloading the VMware Virtual Machine Console on page 104](#).

For more information about consoles, see [Running Virtual Machines](#) in the *VMware GSX Server Virtual Machine Guide*.

Installing VMware GSX Server on a Windows Host

Getting started with VMware GSX Server is simple. The key steps are

1. Install the VMware GSX Server software (including the server, VMware Management Interface, the VmCOM API, the VmPerl API and the VMware Virtual Machine Console) on the server as described in this section.
2. Install the VMware Virtual Machine Console and VMware Scripting APIs on Windows or Linux clients.
3. Start the VMware Virtual Machine Console and enter your serial number. You need to do this only once — the first time you start a console after you install GSX Server.
4. Create a virtual machine using the New Virtual Machine Wizard. See [Creating a New Virtual Machine](#) in the *VMware GSX Server Virtual Machine Guide*.
5. Power on the virtual machine and install a guest operating system. You need the installation media (CD-ROM or floppy disks) for your guest operating system. See [Installing a Guest Operating System](#) in the *VMware GSX Server Virtual Machine Guide*.
6. Install the VMware Tools package in your virtual machine for enhanced performance. See [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide*.
7. Install software in your virtual machine.
8. Start using your virtual machine. Use the VMware Virtual Machine Console, VMware Management Interface and VMware Scripting APIs to manage your server host and virtual machines.

Basic Installation

On a Windows host, you install GSX Server from a master installer. The master installer is a convenient way to install all the components of GSX Server — the server software, the VMware Management Interface and the VMware Scripting APIs — or you can pick and choose which components to install. In addition, the VMware Virtual Machine Console is always installed. All components are installed in their own directories under one master directory.

A basic installation of GSX Server uses two computers — a server hosting a number of virtual machines and a client workstation. The client communicates with the virtual machines on the server over a TCP/IP network link.

In more complex installations, one client can run multiple VMware Virtual Machine Consoles, with each console managing multiple virtual machines on a separate server.

Before you begin, be sure you have:

- A server and host operating system that meet the system requirements for running GSX Server. See [Host System Requirements on page 19](#).
- A remote management client and operating system that meet the system requirements for running the GSX Server remote management software. See [Remote Client Requirements on page 23](#).
- The GSX Server installation software. If you bought a GSX Server media kit, the installation software is on the CD in your package. If you bought the electronic distribution, the installation software is included with the files you downloaded.
- Your GSX Server serial number. The serial number is included in the email message you received from VMware or from the reseller from whom you purchased GSX Server.
- The installation CDs or disks for your guest operating systems.
- If you plan to use the VMware Management Interface, you must make sure Internet Information Services (IIS) is installed and configured properly.

On the Server

A complete installation on the GSX Server host includes:

- The GSX Server package for the server (which includes the tools needed to create and configure virtual machines and the VMware Virtual Machine Console to view and control virtual machines).
- The VMware Management Interface package (a Web server for managing virtual machines and the host from a browser; for more information, see [Managing Virtual Machines and the VMware GSX Server Host on page 99](#)).
- The VmCOM API package, a scripting tool that uses COM to manage virtual machines remotely; for more information, go to www.vmware.com/support/developer.
- The VmPerl API package, a scripting tool that uses Perl to manage virtual machines remotely; for more information, go to www.vmware.com/support/developer.

You can choose a custom installation path where you install only the packages you need.

In most cases, you work directly at the server when you install the server software. You can manage and run virtual machines from the server or from any client.

On a Client Workstation

In addition to a Web browser, you can install the following packages on a client:

- The VMware Virtual Machine Console.
- The VmPerl and VmCOM Scripting APIs (the VmCOM API can be installed only on a Windows client).

These packages are available in the VMware Management Interface and the GSX Server Master Installer (on Windows hosts only). If you are installing the VMware Virtual Machine Console on a Linux client, see [Installing the VMware Virtual Machine Console on a Linux Host on page 67](#).

The VMware Virtual Machine Console can run on a remote client and on the server itself. The VMware Virtual Machine Console is available in client packages for Windows (Windows NT 4.0, Windows 2000, Windows XP and Windows Server 2003) and Linux.

Typically, you run the console and browser on a client. The browser allows access to the VMware Management Interface. The management interface and console let you

- Monitor the operation of virtual machines.
- Start, stop, reset, suspend and resume virtual machines.
- Create and delete virtual machines.
- Configure host and virtual machine settings.

Essentially, the console allows you to manage virtual machines locally and remotely, while the management interface allows you to remotely manage the server host and all the virtual machines on the host.

The VmPerl and VmCOM APIs can connect to Linux and Windows hosts. However, the VmCOM API can run only on a Windows host or client. You can use the APIs to create scripts to automate management of virtual machines and the server host.

Default Directories

By default, the GSX Server components are installed into the following directories:

- The server components and the VMware Virtual Machine Console are installed in `C:\Program Files\VMware\VMware GSX Server`

- The VMware Management Interface components are installed in
C:\Program Files\VMware\VMware Management Interface
- The VmCOM API components are installed in
C:\Program Files\VMware\VMware VmCOM Scripting API
- The VmPerl API components are installed in
C:\Program Files\VMware\VMware VmPerl Scripting API

You can change the directory that contains all the components if you wish, but make note of the new paths you intend to use. The instructions in this manual make use of the default paths.

Installing the GSX Server Software on a Windows Host

You cannot have both VMware GSX Server and VMware Workstation on the same host machine. If you plan to install GSX Server on a host machine that already contains Workstation, you must uninstall the Workstation application first. You cannot install GSX Server on a server that already contains the VMware Virtual Machine Console.

Similarly, you cannot have multiple versions of GSX Server installed on the same host.

If you are upgrading from a previous version of GSX Server, see [Upgrading VMware GSX Server on page 79](#).

1. Log on to your Microsoft Windows host as the Administrator user or as a user who is a member of the Windows Administrators group.

Caution: Do not install GSX Server on a Windows 2000 Server Active Directory domain controller.

Note: On a Windows Server 2003 host, you must be logged on as a local administrator (that is, not logged on to the domain) in order to install GSX Server.

Although you must be logged in as an administrator to install GSX Server, you can run the program after it is installed as a user with normal user privileges.

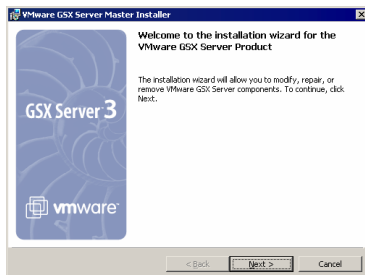
2. Start the GSX Server master installer.

If you are installing from a CD, from the **Start** menu, choose **Run** and enter `D:\Windows\VMware-gsx-server-installer-<xxxx>.exe`, where `D:` is the drive letter for your CD-ROM drive and `<xxxx>` is a series of numbers representing the version and build numbers.

If you are installing from a downloaded file, from the **Start** menu, choose **Run**, browse to the directory where you saved the downloaded installer file (the name is similar to `VMware-gsx-server-installer-<xxxx>.exe`,

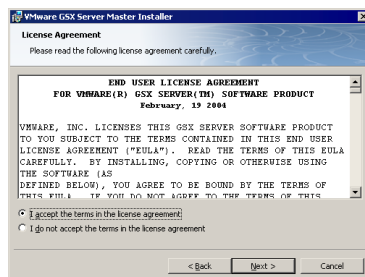
where <xxxx> is a series of numbers representing the version and build numbers).

The master installer starts.



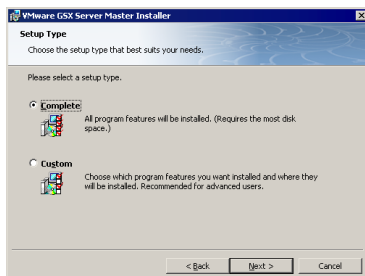
Click **Next**.

3. Accept the end user license agreement (EULA).



Select the **I accept the terms in the license agreement** option, then click **Next**.

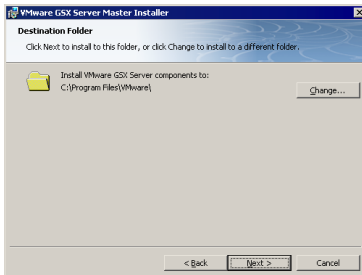
4. Choose whether you want to perform a complete or a custom installation.



Complete Installation

A complete installation installs the server software, the VMware Management Interface, the VMware Virtual Machine Console, the VmCOM API and the VmPerl API on the GSX Server host. To choose the complete installation, select **Complete**, then click **Next**.

If you want to install all the GSX Server components in a directory other than the default, click **Change** and browse to the directory of your choice. If the directory does not exist, the installer creates it for you.



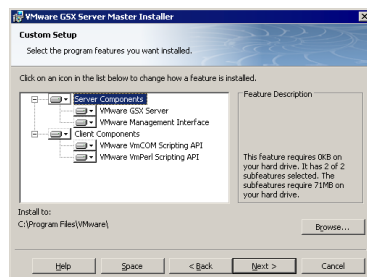
Caution: GSX Server must be installed on a local drive, not a network drive.

Note: Windows and the Microsoft Installer limit the length of a path to a folder to 255 characters for a path to a folder on a local drive and 240 characters for a path to a folder on a mapped or shared drive. If the path to the GSX Server program folder exceeds this limit, an error message appears. You must select or enter a shorter path.

When you are ready to continue, click **Next** and go to step 5.

Custom Installation

A custom installation lets you pick and choose which components to install. You can always run the installer again at a later date to install components you did not install the first time. Select **Custom** and click **Next**. The Custom Setup screen appears.



In the Custom Setup screen, choose the components to install. Click the arrow to the left of the component you do not want to install and select the appropriate option from the menu.

If you need to determine how much free space is on your host, click **Space**. This is useful if you are choosing a custom installation due to limited disk space on your host.

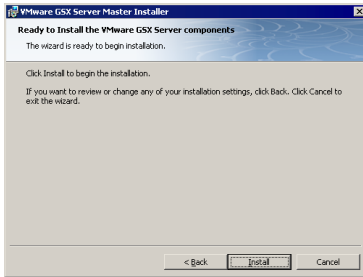
If you want to install all the GSX Server components in a directory other than the default, click **Browse** and select the directory. If the directory does not exist, the installer creates it for you.

Caution: GSX Server must be installed on a local drive, not a network drive.

Note: Windows and the Microsoft Installer limit the length of a path to a folder to 255 characters for a path to a folder on a local drive, and 240 characters for a path to a folder on a mapped or shared drive. If the path to the GSX Server program folder exceeds this limit, an error message appears. You must select or enter a shorter path.

When you are ready to continue, click **Next**.

5. If you want to change any settings or information you provided, now is the time to make those changes. Click **Back** until you reach the screen containing the information you want to change.



Otherwise, click **Install**. The installer begins copying files to your host.

6. If the installer detects that the CD-ROM autorun feature is enabled, you see a message that gives you the option to disable this feature. Disabling it prevents undesirable interactions with the virtual machines you install on this system.
7. Two shortcuts are created for you on your desktop automatically. They give you easy access to virtual machines from the desktop of your host.
8. Click **Finish**. The GSX Server software is installed.



9. If you see a prompt that suggests you reboot your server, do so now to allow GSX Server to complete the installation correctly.

Automating the Installation of GSX Server

To automate the installation of GSX Server, you can use the Microsoft Windows Installer runtime engine to install the software silently (in quiet mode). If you are installing GSX Server on a number of Windows hosts, you may want to use the silent installation features.

The server on which you are installing GSX Server must have Microsoft Windows Installer runtime engine version 2.0 installed. This version is included with Windows Server 2003. If you are installing on a Windows 2000 host (or are installing the VMware Scripting APIs on a Windows NT 4.0 client), check the version of this file:

`%WINDIR%\system32\msiexec.exe`

If you need to upgrade the engine, run `instmsiw.exe`, which is located in the directory where you extract the installation packages; see below.

For more information on using the Microsoft Windows Installer, go to the Microsoft Web site — msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_windows_installer.asp.

To install GSX Server silently on a Windows host, complete the following steps.

1. Extract the individual installation packages. Open a command prompt and on one line type:

```
VMware-gsx-server-installer-<xxxx>.exe /a /s /x /d  
C:\temp\gsx
```

(where `<xxxx>` is a series of numbers representing version and build numbers.)

2. Run the silent installation on the extracted installation packages. At the command prompt, on one line, type:

```
msiexec -i "C:\temp\gsx\VMware GSX Server.msi"  
ADDLOCAL=ALL /qn
```

The installation command can be customized using the following installation properties:

Property Name	Description	Default
DESKTOP_SHORTCUT	Installs GSX Server shortcuts on the desktop. By default, shortcuts are installed on the desktop. To prevent shortcuts from being installed, add the following in step 2: DESKTOP_SHORTCUT = 0	1
DISABLE_AUTORUN	Disables CD autorun on the host. By default, autorun is disabled during the installation. To enable autorun, add the following in step 2: DISABLE_AUTORUN = 0	1

Property Name	Description	Default
REMOVE_LICENSE	Uninstall only: Removes all stored licenses when you uninstall GSX Server. By default, GSX Server keeps the licenses on the server. To remove licenses, add the following in step 2: <pre>REMOVE_LICENSE = 1</pre> Caution: VMware strongly recommends you keep your licenses, in case you reinstall or upgrade your software.	0
SERIALNUMBER	Automatically enters the serial number. To enter the serial number, add the following in step 2: <pre>SERIALNUMBER=<serialNumber></pre>	none

The `ADDLOCAL` option defaults to install all GSX Server components. You can customize the installation using a combination of the `ADDLOCAL` and `REMOVE` options. You can add or remove the following components:

- **ALL**, which includes all the options in this list.
- **Network**, which includes the bridged networking adapter (`vmnet0`), the host-only networking adapter (`vmnet1`) and the NAT networking adapter (`vmnet8`). It also includes **NAT** and **DHCP**, but these can be removed from the installation.
- **NAT**, the VMware NAT Service.
- **DHCP**, the VMware DHCP Service.

To include a component, use it with the `ADDLOCAL` option.

To exclude a component, use it with the `REMOVE` option. You always install the bridged and host-only network adapters as part of the **Network** component.

For example, to install everything but the VMware NAT and DHCP services, specify on the command line:

```
ADDLOCAL=ALL REMOVE=DHCP,NAT
```

Note: The DHCP and NAT components are children of the **Network** component. Thus, you also skip installation of the VMware NAT and DHCP services if you specify:

```
ADDLOCAL=ALL REMOVE=Network
```

Installing VMware GSX Server on a Linux Host

Getting started with VMware GSX Server is simple. The key steps are

1. Install the GSX Server software (including the server, VMware Management Interface, the VMware Virtual Machine Console and the VmPerl API) on the server.
2. Install the VMware Virtual Machine Console and VMware Scripting APIs on Windows or Linux clients.
3. Start the VMware Virtual Machine Console and create a virtual machine using the New Virtual Machine Wizard. See [Creating a New Virtual Machine](#) in the *VMware GSX Server Virtual Machine Guide*.
4. Power on the virtual machine and install a guest operating system in the new virtual machine. You need the installation media (CD-ROM or floppy disks) for your guest operating system. See [Installing a Guest Operating System](#) in the *VMware GSX Server Virtual Machine Guide*.
5. Install the VMware Tools package in your virtual machine for enhanced performance. See [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide*.
6. Install software in your virtual machine.
7. Start using your virtual machine. Use the VMware Virtual Machine Console, VMware Management Interface and VMware Scripting APIs to manage your server host and virtual machines.

Basic Installation

A basic installation of GSX Server uses two computers — a server, hosting a number of virtual machines, and a client workstation. The client communicates with the virtual machines on the server over a TCP/IP network link.

In more complex installations, one client can run multiple VMware Virtual Machine Consoles, with each console managing multiple virtual machines on a separate server. And consoles on multiple clients can connect to virtual machines on any server.

Before you begin, be sure you have:

- A server and host operating system that meet the system requirements for running GSX Server. See [Host System Requirements on page 19](#).

- A remote management client and operating system that meet the system requirements for running the GSX Server remote management software. See [Remote Client Requirements on page 23](#).
- The installation CDs or disks for your guest operating systems.
- The GSX Server installation software. If you bought a GSX Server media kit, the installation software is on the CD in your package. If you bought the electronic distribution, the installation software is in the files you downloaded.
- Your GSX Server serial number. The serial number is included in the email message you received from VMware or from the reseller from whom you purchased GSX Server.

Also, before you install and run VMware GSX Server, check the following notes and make any necessary adjustments to the configuration of your host operating system.

- The real-time clock function must be compiled into your Linux kernel.
- GSX Server for Linux systems requires that the parallel port PC-style hardware option (`CONFIG_PARPORT_PC`) be built and loaded as a kernel module (that is, it must be set to `m` when the kernel is compiled).
- **(SuSE Linux 7.1 and later hosts):** The `inetd` process must be configured to start when the host operating system boots. See [Before You Install on a SuSE Linux 7.1 or Later Host on page 59](#).
- **(SuSE Linux Enterprise Server 8 hosts):** The `gcc` package must be installed on your host before you install GSX Server. See [Before You Install on a SuSE Linux Enterprise Server 8 Host on page 60](#).

Caution: Some operating systems, such as Red Hat Linux 7.2 and 7.3, include a firewall by default. This firewall prevents access from the VMware Virtual Machine Console and the VMware Management Interface on client computers to the GSX Server host. In order for the VMware Virtual Machine Console to connect to the host, you need to open up port 902. To connect to the host with the VMware Management Interface, you need to open up port 8333 (and port 8222 if you plan to disable SSL for the management interface).

On the Server

You can install up to three software packages on the Linux server:

- The GSX Server package for the server (from an RPM or tar archive available on the GSX Server CD-ROM or the VMware Web site). The RPM file is called `VMware-gsx-<xxx>.i386.rpm` while the tar archive is called

`VMware-gsx-<xxxx>.tar.gz`, where `<xxxx>` is a series of numbers representing the version and build numbers.

Note: The VmPerl API package is installed when you install the server software. The VmPerl API is a scripting tool that uses Perl to manage virtual machines remotely; for more information, go to www.vmware.com/support/developer/.

- The VMware Management Interface package (from a tar archive available on the GSX Server CD-ROM or the VMware Web site). This tar archive is called `VMware-mui-<xxxx>.tar.gz`.
- The VMware Virtual Machine Console package (which you download from the VMware Management Interface; the package is also available as an RPM file or tar archive in a client GZip file that also contains the VmPerl API, available on the GSX Server CD-ROM or from the VMware Web site). The RPM file is called `VMware-console-<xxxx>.i386.rpm` while the tar archive is called `VMware-console-<xxxx>.tar.gz`.

In most cases, you work directly at the server when you install the server software. You can manage and run virtual machines from the server or from any client.

On a Client Workstation

In addition to a Web browser, you can install the following packages on a client:

- The VMware Virtual Machine Console.
- The VmPerl and VmCOM Scripting APIs (the VmCOM API can be installed only on a Windows client); for more information, go to www.vmware.com/support/developer/.

These packages are available in the VMware Management Interface. If you are installing the VMware Virtual Machine Console on a Windows client, see [Installing the VMware Virtual Machine Console on a Windows Host on page 64](#).

VMware Virtual Machine Consoles can run on clients and on the server itself. Console packages are available for Windows (Windows NT 4.0, Windows 2000, Windows XP and Windows Server 2003) and Linux.

Typically, you run the console and browser on a client. The browser allows access to the VMware Management Interface. The management interface and console let you

- Monitor the operation of virtual machines.
- Start, stop, reset, suspend and resume virtual machines.
- Create and delete virtual machines.
- Configure host and virtual machine settings.

Essentially, the console allows you to manage virtual machines locally and remotely, while the management interface allows you to remotely manage the server host and all the virtual machines on the host.

The VmPerl and VmCOM Scripting APIs can connect to Linux and Windows hosts. However, the VmCOM API can run only on a Windows client. You can use the APIs to create scripts to automate management of virtual machines and the host.

Default Directories

By default, the GSX Server components are installed into the following directories:

- The server components are installed in
`/usr/bin`
- The VMware Management Interface components are installed in
`/usr/lib/vmware-mui`
- The VMware Virtual Machine Console components are installed in
`/usr/bin`
- The Apache server components are installed in
`/usr/lib/vmware-mui/apache/bin`
(so they do not conflict with existing Apache software on your server)
- The VmPerl API executable files are installed in
`/usr/bin`
- The VmPerl API library files are installed in
`/usr/lib/vmware-api`

If you installed the software from a tar installer, you can change these paths if you wish, but make note of the new paths you intend to use. The instructions in this manual make use of the default paths.

Installing the GSX Server Software on a Linux Host

The steps below describe an installation on a Red Hat Linux host from a CD-ROM. If you downloaded the software, the steps are the same except that you start from the directory where you saved the downloaded installer file, not from the CD. If you are using a different Linux distribution, some of the commands may be different.

You cannot have both VMware GSX Server and VMware Workstation on the same host machine. If you plan to install GSX Server on a host machine that already contains Workstation, the Workstation application is automatically upgraded to GSX Server.

Before you install the GSX Server software, ensure your Linux distribution is for a **server**, not a workstation. If you are running a workstation distribution, you need to install the `inetd` process in order to connect to the VMware Virtual Machine Console and VMware Management Interface. If you need to, review the [Host System Requirements on page 19](#).

Upgrade Note: If you are upgrading from an earlier version of GSX Server to a later one, the choices you made during the earlier installation become the defaults for the new installation. As a result, you may see options that are different from those described below. For more information, see [Upgrading VMware GSX Server on page 79](#).

1. Log on to your Linux host with the user name you plan to use when running VMware GSX Server.
2. In a terminal window, become root so you can perform the initial installation.
`su -`
3. Mount the CD-ROM drive and change to the `Linux` directory on the CD.
`mount /dev/cdrom /mnt/cdrom`
`cd /mnt/cdrom/Linux`
4. Do one of the following:

- **Use the RPM installer:** Run RPM specifying the installation file.
`rpm -Uhv VMware-gsx-<xxx>.i386.rpm`
(`VMware-gsx-<xxx>.i386.rpm` is the installation file on the CD; where `<xxx>` is a series of numbers representing version and build numbers.)

Note: If you are upgrading from VMware GSX Server 2, you must take a special step before you install the RPM package. You need to remove the prebuilt modules RPM package included in the version 2 release. To remove the modules, type the following at a command prompt:

```
rpm -e VMwareGSXKernelModules
```

- **Use the tar installer:** Complete the following steps.
 - a. Copy the tar archive to a directory on your hard drive — for example, to `/tmp`.
`cp VMware-gsx-<xxx>.tar.gz /tmp`
(where `<xxx>` is a series of numbers representing the version and build numbers)
 - b. Change to the directory to which you copied the file.
`cd /tmp`

c. Unpack the archive.

```
tar xzf VMware-gsx-<xxxx>.tar.gz
```

d. Change to the installation directory.

```
cd vmware-gsx-distrib
```

e. Run the installation program.

```
./vmware-install.pl
```

f. Accept the default directories for the binary files, daemon files, library files, manual files, documentation files, `init` directories and `init` scripts.

5. Run the configuration program.

```
vmware-config.pl
```

Note: If you are installing GSX Server on a Mandrake host, the configuration program asks for the location of `lspci`. When that prompt appears, enter the following path:

```
/usr/bin/lspcidrake
```

Note: If you use the RPM installer, you need to run this program separately from the command line. If you install from the tar archive, the installer offers to launch the configuration program for you. Answer Yes when you see the prompt.

Use this program to reconfigure GSX Server whenever you upgrade your kernel. It is not necessary to reinstall GSX Server after you upgrade your kernel.

You can also use `vmware-config.pl` to reconfigure the networking options for VMware GSX Server — for example, to add or remove host-only networks.

6. Press Enter to read the end user license agreement (EULA). You may page through it by pressing the space bar. If the `Do you accept` prompt doesn't appear, press Q to get to the next prompt.

7. Configure networking for your virtual machines.

- If you want to use any type of networking with virtual machines, answer Yes to this prompt: `Do you want networking for your virtual machines?`

Bridged networking is always enabled if you enable networking. For more information about bridged networking, see [Bridged Networking](#) in the *VMware GSX Server Virtual Machine Guide*.

- To enable NAT, answer Yes to the following prompts:
`Do you want to be able to use NAT networking in your virtual machines?`

Do you want this script to probe for an unused private subnet?

This allows you to connect your virtual machines to an external network when you have only one IP network address on the physical network, and that address is used by the host computer. For more information, see [Network Address Translation \(NAT\)](#) in the *VMware GSX Server Virtual Machine Guide*.

- To enable host-only networking, answer Yes to the following prompts:
Do you want to be able to use host-only networking in your virtual machines?
Do you want this script to probe for an unused private subnet?

Host-only networking allows for networking between the virtual machine and the host operating system. For more information, see [Host-Only Networking](#) in the *VMware GSX Server Virtual Machine Guide*.

8. Specify the port the VMware Virtual Machine Console uses when connecting to the GSX Server host remotely. Port 902 is the default port. If your site uses this port for another application — for example, `ideafarm-chat` uses this port — then specify a different port for the console to use here. To change the port later, see [Changing the Port Number for VMware Virtual Machine Console Connections on page 101](#).
9. If you are upgrading from an earlier version of GSX Server, the following prompt appears: Do you want the installer to set up permissions for your registered virtual machines? This will be done by setting new permissions on all files found in `/etc/vmware/vm-list`.

Type `y`. The following permissions are set for all registered virtual machines:

- **Read, write** and **execute** — for the user who created the virtual machine (the owner)
 - **Read** and **execute** — for the primary group to which the owner belongs
 - **Read** — for users other than the owner or a member of the owner's group
10. Specify the directory where you want to store your virtual machine files. By default, this directory is `/var/lib/vmware/Virtual Machines`. Make sure this location is on a large enough file system to contain the files, as the virtual disk files for each virtual machine are usually are gigabytes in size.

11. Enter your GSX Server serial number exactly as it appears (with hyphens) in the email message you received from VMware or from the reseller from whom you purchased GSX Server. When you enter the serial number, it is saved in your license file.
12. The configuration program displays a message saying the configuration completed successfully. If it does not display this message, run the configuration program again.
13. When you finish, do one of the following:
 - Log out of the root account.
`exit`
 - Install the VMware Management Interface. Go to step 3 under [Installing the VMware Management Interface on a Linux Host on page 58](#).
 - Install the VMware Virtual Machine Console. Go to step 3 under [Installing the VMware Virtual Machine Console on a Linux Host on page 67](#).

Installing the VMware Management Interface on a Linux Host

The steps below describe an installation of the VMware Management Interface on a Red Hat Linux host from a CD-ROM. If you downloaded the software, the steps are the same except that you start from the directory where you saved the installer file you downloaded, not from the CD. If you are using a different Linux distribution, some commands may be different.

Note: You must install the `libdb.so.3` library from your Linux CD-ROM first. For more information, see [Before You Install the VMware Management Interface on a Linux Host on page 60](#).

1. In a terminal window, if you haven't done so already, become root so you can carry out the installation.
`su -`
2. Mount the CD-ROM drive and change to the `Linux` directory on the CD.
`mount /dev/cdrom /mnt/cdrom`
`cd /mnt/cdrom/Linux`
3. Copy the tar archive to a directory on your hard drive (for example, to `/tmp`).
`cp VMware-mui-<xxx>.tar.gz /tmp`
(where `<xxx>` is a series of numbers representing version and build numbers)

Caution: Make sure the directory to which you plan to untar the tar archive does not contain any files from a previous management interface tar installation.

Change to the directory to which you copied the file.

`cd /tmp`

Unpack the archive.

`tar xzf VMware-mui-<xxx>.tar.gz`

(where `<xxx>` is a series of numbers representing version and build numbers)

4. Change to the installation directory.
`cd vmware-mui-distrib`
5. Run the installation program.
`./vmware-install.pl`
6. Press Enter to continue.
7. Accept the EULA.
8. Specify the directory where you want to install the management components, the binary files, management interface files, `init` directories and `init` scripts. Or accept the default directories.

9. Allow the configuration program `vmware-config-mui.pl` to run.
10. Specify the number of minutes before a management interface session times out. The default session length is 60 minutes.
11. When you finish, you can:
 - Log out of the root account.
`exit`
 - Install the VMware Virtual Machine Console. Go to [page 67](#).

Installing an X Server

You need an X server to run the VMware Virtual Machine Console. If an X server is not installed, you must install `libxpm.so.4`, located on your Linux distribution disk.

Before You Install on a SuSE Linux 7.1 or Later Host

The `inetd` process, which is required for the VMware Management Interface and the VMware Virtual Machine Console to run properly, is not configured to start at boot time on SuSE Linux 7.1 and later hosts.

Before you install GSX Server on a SuSE Linux 7.1 or later host system, you need to configure your SuSE Linux 7.1 or later host so that the `inetd` process starts at boot time. Boot the host operating system and make sure the network card and disk subsystem work as expected.

Configuring the `inetd` Process in the Host Operating System

1. Start your X server, if it does not start by default, and log in as the root user.
2. Run `YAST2`, the default configuration utility for SuSE Linux 7.2 and later.
3. Click **Network** (SuSE Linux 7.1) or **Network/Basic** (SuSE Linux 7.2 or later), then click **Start/stop services (inetd)**.
4. Select the **On with default configuration** option.
5. Click **Finish**, then click **Close** to exit `YAST2`. The `inetd` process automatically starts when you reboot the host operating system.

Before You Install on a SuSE Linux Enterprise Server 8 Host

The `gcc` program is not installed on a SLES 8 host by default. This compiler is required by the VmPerl API.

Before you install GSX Server on a SLES 8 host system, you must install `gcc`.

Installing gcc in the Host Operating System

1. Start your X server, if it does not start by default, and log in as the root user.
2. Run `YAST2`, the default configuration utility for SLES 8.
3. Click **Software** in the left pane, click **Install or remove software** in the right pane.
4. Check **C++ Compiler and Tools** in the left pane, then click **Accept**.
5. When prompted, insert the SLES 8 CD.
6. Click **Close** to exit `YAST2`. The `gcc` program is installed. Now install GSX Server.

Before You Install the VMware Management Interface on a Linux Host

If you are running GSX Server on a Linux host, you must install the `libdb.so.3` library from your Linux distribution's CD-ROM before you install the VMware Management Interface. The version that comes with a default Linux installation is incompatible with the management interface and returns the following error when you start the management interface:

```
Couldn't find necessary components on your system. It
appears that you are missing the following library:
libdb.so.3.
```

New versions of Red Hat Linux (8.0+) are known to ship without these libraries. If you are running Red Hat 8.0 or greater, please install this rpm: `compat-db-3.3-<###> rpm` (where **<###>** is a version number particular to your version of the distribution from your installation CD).

If you are running a distribution other than Red Hat, please contact your vendor for a suitable library. Once the package has been installed, you may start GSX Server with the following command:

```
/home/vmware/mui/apache/bin/apachectl/start
```

To install the correct library, run the `compat-db-3.3-<###>.i386.rpm` RPM package. If you installed this package after you installed the management interface software, start the management interface's Apache server with this command:

```
/etc/init.d/httpd.vmware start
```

Configuring Web Browsers for Use with GSX Server

If you intend to run the VMware Management Interface in Internet Explorer 6.0 on a Windows system, you must take certain steps to configure Internet Explorer properly. These steps are needed whether the browser is running on a GSX Server Windows host or you are using a Windows client machine to connect to a GSX Server host.

In order to run the GSX Server in-product help from a console on a Linux system, you may need to link to the location of Netscape on the system, if it is different from the location where GSX Server expects it to be.

The configuration steps allow you to perform the following activities:

- [Launching the VMware Virtual Machine Console from the Management Interface on an Encrypted Server on page 61](#)
- [Connecting to the Management Interface on a Proxy Server on page 62](#)
- [Launching Help in Netscape on a Linux System on page 63](#)

Launching the VMware Virtual Machine Console from the Management Interface on an Encrypted Server

You can launch the VMware Virtual Machine Console from the VMware Management Interface automatically. In order to do this in an Internet Explorer 6.0 browser on a Windows system where SSL is encrypting your GSX Server remote connections, you must ensure that the **Do not save encrypted pages to disk** option is disabled.

For information on encrypting remote connections, see [Enabling and Disabling SSL for Remote Sessions on page 114](#).

When this option is enabled, Internet Explorer does not save any files to disk, including the files it needs to hand off to helper applications. This prevents the console from launching automatically.

Caution: This option may have been enabled deliberately at your site to prevent the saving of sensitive files to disk. Disabling it may permit other sensitive information to be saved to disk.

Caution: Some patches installed when you run Windows Update reset this setting, so you may need to repeat this process after you run Windows Update.

To disable the option, complete the following steps.

1. In the Internet Explorer 6.0 window, open the Internet Options control panel. Choose **Tools > Internet Options**.
2. Click the **Advanced** tab.
3. Scroll down to the Security section and uncheck **Do not save encrypted pages to disk**.
4. Click **OK**.

Connecting to the Management Interface on a Proxy Server

If your network is protected behind a proxy server, there are certain steps you must take in order to use the management interface in Internet Explorer 6.0 on a Windows system. Follow the steps for the appropriate Windows operating system.

Windows Server 2003 Systems

1. Launch Internet Explorer 6.0.
2. Choose **Tools > Internet Options**, then click the **Security** tab.
3. Select **Trusted sites**, then click **Sites**.
4. In the **Add this Web site to the zone** entry field, type
`https://*.<domain>.com`
(where <domain> is your organization's domain name).
5. Click **Add**.
6. Click **OK** until you return to the browser window.

When you use Internet Explorer 6.0 to connect to the management interface, be sure to use fully qualified domain names.

Windows Systems Other than Windows Server 2003

Follow these steps for Windows 2000, Windows XP and Windows NT operating systems.

1. Launch Internet Explorer 6.0.
2. Choose **Tools > Internet Options**.
3. Click the **Connections** tab, then click **LAN Settings**.
4. Make sure that **Bypass proxy server for local addresses** is checked.
5. Click **OK** until you return to the browser window.

When you use Internet Explorer 6.0 to connect to the management interface, do **not** use fully qualified domain names.

Connecting to the Management Interface When There Is No Proxy Server

If you are on a Windows system and your network does not use a proxy server, you must use fully-qualified domain names when connecting to the management interface with Internet Explorer 6.0.

Launching Help in Netscape on a Linux System

To use VMware GSX Server Help on a Linux system, you must have a Web browser installed on your physical computer. GSX Server expects to find the Netscape browser in `/usr/bin/netscape`. If this matches the configuration of your host computer, you do not need to take any special steps. If you are using a different browser or if your Netscape browser is in a different location, add a symbolic link to it from `/usr/bin`.

```
ln -s <path to browser> /usr/bin/netscape
```

Installing the VMware Virtual Machine Console

The VMware Virtual Machine Console enables you to view and control GSX Server virtual machines from a remote client or on the server host. Multiple users can use the console to connect to a virtual machine from the server host or from remote clients at the same time. Use the instructions below that correspond to the operating system running on your system.

Consoles can also be launched from the VMware Management Interface. If you use Netscape or Mozilla as your browser, you need to configure the MIME type for the console. To set the MIME type, see [Setting a MIME Type to Launch the VMware Virtual Machine Console on page 157](#). Internet Explorer is automatically configured when you install the console software.

Caution: Do not install a console from a client installer package onto the GSX Server 3 host. Do not download and install a console from an older version of GSX Server or ESX Server onto any client.

Installing the VMware Virtual Machine Console on a Windows Host

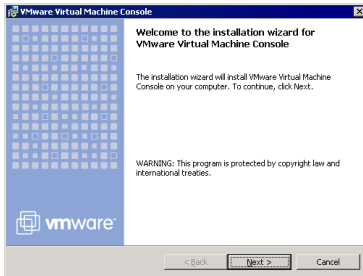
On the GSX Server for Windows host, the VMware Virtual Machine Console is installed automatically from the master installer when you installed the GSX Server component. If you need to upgrade the console on the GSX Server host, use the master installer.

You can download the installer from the VMware Management Interface or find it on the GSX Server installation CD-ROM in the Windows client package. You can run this console on the GSX Server host or any Windows client.

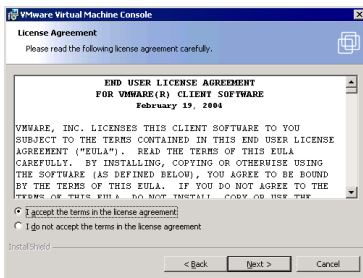
To download the console from the management interface, see [Downloading the VMware Virtual Machine Console on page 104](#).

1. After you download the console installation package, go to the directory where you downloaded the installer and run `VMware-console-<xxxx>.exe`,

where <xxxx> is a series of numbers representing the version and build numbers. The InstallShield Wizard dialog box appears. Click **Next**.

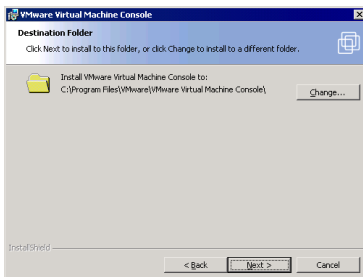


2. Accept the end user license agreement (EULA).

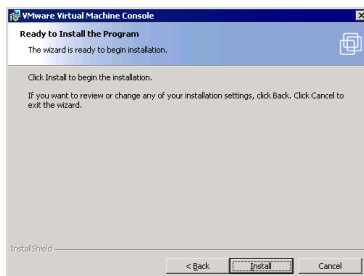


Select **I accept the terms in the license agreement**, then click **Next**.

3. Choose the directory in which to install the console. If you prefer to install it in a directory other than the default, click **Change** and change to your directory of choice. If the directory does not exist, it is created for you. Click **Next**.

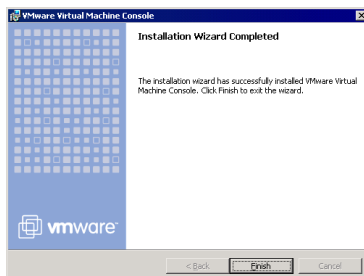


4. If you want to change any settings or information you provided, now is the time to make those changes. Click **Back** until you reach the dialog box containing the information you want to change.



Otherwise, click **Install**. The installer begins copying files to your host.

5. When the setup completes, click **Finish**. You do not need to reboot your host operating system after you install the console.



Installing the VMware Virtual Machine Console on a Linux Host

The steps below describe an installation of the VMware Virtual Machine Console on a Red Hat Linux host from a CD-ROM. If you downloaded the software, the steps are the same except that you start from the directory where you saved the installer file you downloaded, not from the CD. If you are using a different Linux distribution, some commands may be different.

You can download the VMware Virtual Machine Console installer from the VMware Management Interface or find it on the GSX Server installation CD-ROM in the Linux client package. You can run this console on the GSX Server host or any Linux client.

To download the console from the management interface, see [Downloading the VMware Virtual Machine Console on page 104](#).

1. In a terminal window, if you have not done so already, become root so you can carry out the installation steps.

```
su -
```

2. Mount the CD-ROM drive and change to the `Linux` directory on the CD.

```
mount /dev/cdrom /mnt/cdrom
cd /mnt/cdrom/Linux
```

3. Unzip the client installer archive to `/tmp`.

```
unzip VMware-gsx-server-linux-client-<xxxx>.zip -d /tmp
```

(where **<xxxx>** is a series of numbers representing the version and build numbers)

Caution: If you intend to install the VMware Virtual Machine Console from a tar package, make sure the directory to which you plan to untar the tar archive does not contain any files from a previous console tar installation.

4. Change to the `/tmp` directory.

```
cd /tmp
```

5. Do one of the following:

- **Use the RPM installer.** Run RPM specifying the installation file.

```
rpm -Uvh VMware-console-<xxxx>.i386.rpm
```

(where **<xxxx>** is a series of numbers representing the version and build numbers)

- **Use the tar installer.** Complete the following steps.

- a. Unpack the archive.

```
tar xzf VMware-console-<xxxx>.tar.gz
```

(where <xxxx> is a series of numbers representing the version and build numbers)

The archive unpacks to `vmware-console-distrib`.

- b. Run the installer.

```
cd vmware-console-distrib
./vmware-install.pl
```

- c. Accept the EULA and answer the questions specifying default directories for the binary files, library files, manual files and documentation files.

- d. If the `Do you accept` prompt doesn't appear, press `Q` to continue.

6. Run the configuration program `vmware-config-console.pl`.

Note: If you use the RPM installer, you need to run this program separately from the command line. If you install from the tar archive, the installer offers to launch the configuration program for you. Answer Yes when you see the prompt.

You see the following prompt: `What port do you want the remote console to use to connect to server. [902]`

If you specified a different port number when you installed the server software, enter that port number here. Otherwise, keep the default of 902.

7. When you finish, log out of the root account.

```
exit
```

Installing the VMware Scripting APIs

VMware GSX Server supports the VMware Scripting APIs, which include the VmPerl Scripting API and the VmCOM Scripting API. You can use the VMware Scripting APIs to manage the GSX Server host and virtual machines locally and remotely.

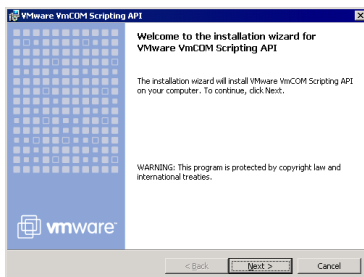
For more information, go to www.vmware.com/support/developer.

Installing the VmPerl and VmCOM Scripting APIs on a Windows Host

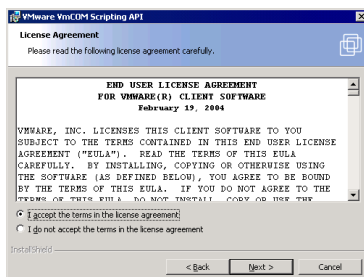
On either a Windows server host or a Windows remote computer, you can use either the VmPerl API or the VmCOM API. Both scripting APIs are installed automatically on the GSX Server for Windows host from the master installer if you chose a complete installation. In addition, you can make the APIs available for download by customizing the download menu on the Login page of the VMware Management Interface. For more information, see [Downloading the VMware Virtual Machine Console on page 104](#).

You have a choice of installing either the VmCOM or the VmPerl API, or both.

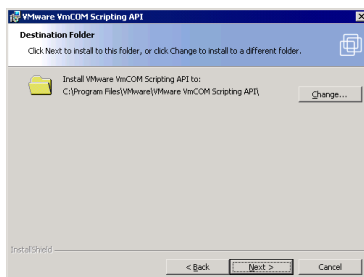
1. Choose **Start > Run** and browse to the directory where you saved the downloaded installer file (the name is similar to `VMware-VmPerlAPI-<xxxx>.exe` or `VMware-VmCOMAPI-<xxxx>.exe`, where `<xxxx>` is a series of numbers representing the version and build numbers).
2. The installer starts. Click **Next**.



- Acknowledge the end user license agreement (EULA). Select **I accept the terms in the license agreement**, then click **Next**.

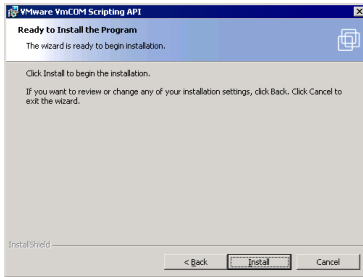


- Choose the directory in which to install the scripting API. To install it in a directory other than the default, click **Change** and browse to your directory of choice. If the directory does not exist, the installer creates it for you. Click **Next**.



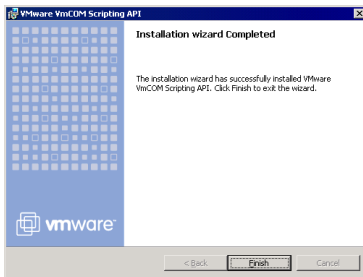
Note: Windows and the Microsoft Installer limit the path length to 255 characters for a path to a folder on a local drive, and 240 characters for a path to a folder on a mapped or shared drive. If the path to the scripting API program folder exceeds this limit, an error message appears. You must select or enter a shorter path.

5. If you want to change any settings or information you provided, now is the time to make those changes. Click **Back** until you reach the dialog box containing the information you want to change.



Otherwise, click **Install**. The installer begins copying files to your host.

6. Click **Finish**. The VMware Scripting API is installed.



If you install the VmCOM API, two directories named `MiniMUI` and `SampleScripts` are created in the VmCOM API directory. The `MiniMUI` directory contains a sample Microsoft Visual Basic 6 project that uses the VmCOM API. The `SampleScripts` directory contains VBScript and JScript samples using the VmCOM API.

If you install the VmPerl API, a `SampleScripts` directory is created in the VmPerl API directory. The `SampleScripts` directory contains sample scripts using the VmPerl API.

Installing the VmPerl API on a Linux Host

On either a Linux server host or a Linux remote computer, you can use only the VmPerl API. The VmCOM API cannot be installed on a Linux host, although the VmCOM API installed on a Windows remote client can communicate with a Linux host. You can make the VmPerl API tar archive available for download by customizing the download menu on the Login page of the VMware Management Interface. See [Downloading the VMware Virtual Machine Console on page 104](#).

1. Download the VmPerl API package from the VMware Management Interface Login page to the machine on which you want to run the VMware Scripting API.
2. In a terminal window, if you have not done so already, become root so you can carry out the installation steps.
`su -`
3. Untar the package.
`tar xzf VMware-VmPerlAPI-<xxxx>.tar.gz`
 (where <xxxx> is a series of numbers representing the version and build numbers)
4. Change to the installation directory.
`cd vmware-api-distrib`
5. Run the installation program.
`./vmware-install.pl`
6. Press Enter to read the end user license agreement (EULA). You may page through it by pressing the spacebar. If the `Do you accept?` prompt doesn't appear, press `Q` to get to the next prompt. Accept the EULA.
7. Specify the directory where you want to install the VmPerl API executable files. The default is where Perl is installed on your host, typically `/usr/bin`.
8. Specify the directory where you want to install the VmPerl API library files. The default is `/usr/lib/vmware-api`.
 This directory includes the sample scripts for the VmPerl API. The `sampleScripts` directory contains example scripts that demonstrate use of the VmPerl API. You may customize these scripts for your particular organization.
9. Specify the directory where you want to install the VmPerl API documentation files. These files consist of the README, end user license agreement and copyright information. The default is `/usr/share/doc/vmware-api`.
10. When you finish, log out of the root account.
`exit`

Uninstalling VMware GSX Server

The following sections describe how to remove the GSX Server components from your system. Follow the steps for your host operating system.

Uninstalling GSX Server on a Windows Host

To uninstall GSX Server, complete the following steps. These steps remove all the components you installed with the GSX Server master installer, including the server software, the VMware Management Interface and the VMware Scripting APIs.

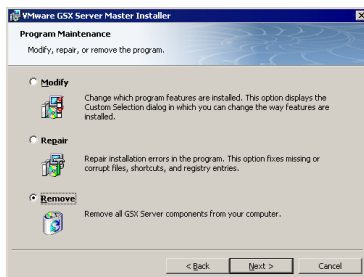
To uninstall the VMware Virtual Machine Console, see [Uninstalling the VMware Virtual Machine Console on a Windows Host on page 77](#).

If you chose the custom installation path, any components you installed at that time are removed when you use the master installer to uninstall GSX Server.

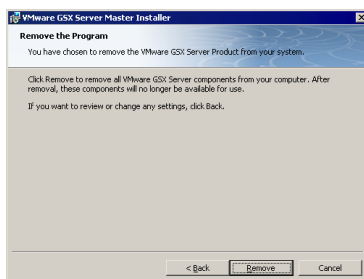
1. On a Windows Server 2003 host, choose **Start > Settings > Control Panel > Add or Remove Programs**. Select the **VMware GSX Server Installer** and click **Change**.
On a Windows 2000 host, choose **Start > Settings > Control Panel > Add/Remove Programs**. Select the **VMware GSX Server Installer** and click **Change**.
2. After the master installer launches, click **Next**.



3. Select **Remove**, then click **Next**.

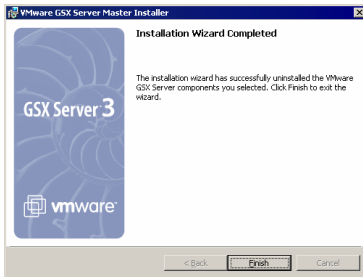


4. When you are ready to begin removing GSX Server, click **Remove**.



5. During the uninstallation, you are asked whether you want to keep your VMware licenses in the Windows registry. VMware strongly recommends you keep your licenses, in case you reinstall or upgrade your software. To keep the licenses in the registry, click **Yes**. The uninstallation continues.
6. During the uninstallation, you are asked whether you want to keep any login information for any virtual machines configured to run as specific user accounts. If you choose to delete the login information, then reinstall GSX Server, any virtual machines configured to run as specific users will run as the user that powers on those virtual machines. After you decide whether or not to keep the login information, the uninstallation continues.

- After all the components are removed, click **Finish**.



- If you see a prompt that suggests you reboot your server, do so now to allow GSX Server to complete the uninstallation correctly.

Removing Selected Components on a Windows Host

With the master installer, you can choose to remove specific components from your GSX Server installation. For example, if you decide to not use the VmPerl API, you can remove only that component.

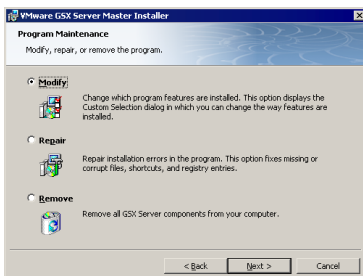
Note: Do not use this method to remove GSX Server. Use it to remove the VMware Scripting APIs or the VMware Management Interface **only**.

To remove a component, complete the following steps.

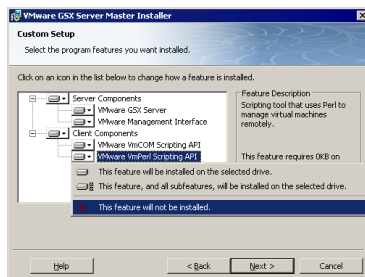
- On a Windows Server 2003 host, choose **Start > Settings > Control Panel > Add or Remove Programs**. Select the **VMware GSX Server Installer** and click **Change**.

On a Windows 2000 host, choose **Start > Settings > Control Panel > Add/Remove Programs**. Select the **VMware GSX Server Installer** and click **Change**.

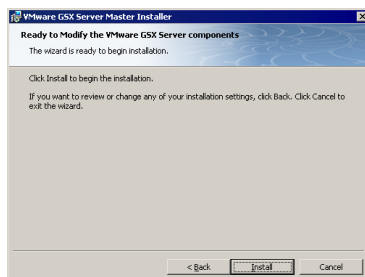
- After the master installer launches, click **Next**. The Program Maintenance screen appears.



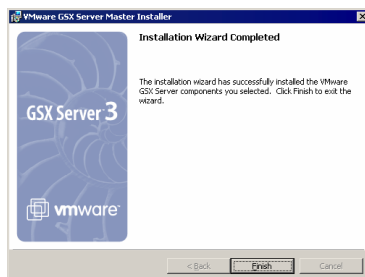
3. Select **Modify**, then click **Next**. The Custom Setup screen appears.



4. Click the arrow to open the menu next to the component you want to remove, select **This feature will not be installed**, then click **Next**.



5. When you are ready to begin removing the component, click **Install**.
6. After the component is removed, click **Finish**.



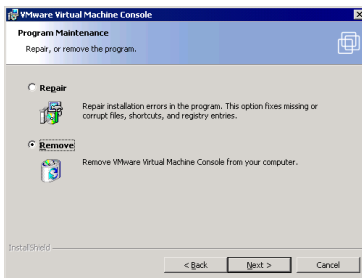
Uninstalling the VMware Virtual Machine Console on a Windows Host

To uninstall the console on a Windows host, use Add/Remove Programs in the Windows Control Panel.

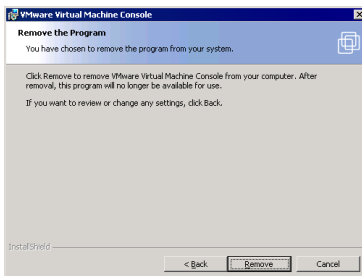
1. Choose **Start > Settings > Control Panel**.
2. Double-click **Add/Remove Programs** (Add or Remove Programs on a Windows Server 2003 host).
3. Select **VMware Virtual Machine Console**, then click **Change**.

Note: If the console was installed on Windows NT 4.0, click **Add/Remove**.

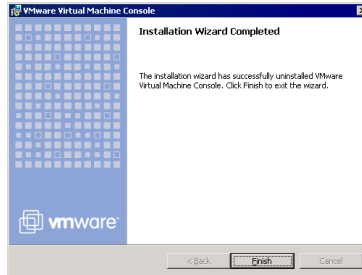
4. A wizard starts. Click **Next**.



5. In the next screen, select **Remove**, then click **Next**.



6. To start removing the console, click **Remove**.



7. After the wizard finishes removing the console, click **Finish**. You do not need to reboot the system after you remove the console.

Uninstalling GSX Server on a Linux Host

To uninstall any GSX Server component, open a terminal and log in as the root user.

If you used the RPM installer to install GSX Server, remove the software from your system by running

```
rpm -e VMware-gsx
```

If you used the tar installer to install GSX Server, remove the software from your system by running

```
vmware-uninstall.pl
```

Note: Uninstalling the server software removes the VmPerl API installed with it.

To uninstall the VMware Management Interface components, run the program

```
/usr/bin/vmware-uninstall-mui.pl
```

To uninstall a Linux console that was installed from an RPM package, type the following

```
rpm -e VMware-console
```

To uninstall a Linux console that was installed from a tar package, run the program

```
/usr/bin/vmware-uninstall-console.pl
```

To uninstall the VmPerl API that was installed on a remote client from a client package, type the following

```
/usr/bin/vmware-uninstall-api.pl
```

3

CHAPTER

Upgrading VMware GSX Server

The following sections describe how to upgrade VMware GSX Server on your Linux or Windows host system and how to use virtual machines created under earlier versions of GSX Server with the current version:

- [Preparing for the Upgrade on page 80](#)
- [Upgrading on a Windows Host on page 83](#)
- [Upgrading on a Linux Host on page 84](#)
- [Using Virtual Machines Created with Version 2 under Version 3 on page 85](#)
- [Using Virtual Machines Created with Version 1 under Version 3 on page 95](#)

Preparing for the Upgrade

Before You Install VMware GSX Server

There are a few steps you should take — before you remove an already installed version of GSX Server and install the new version of GSX Server — to ensure the best possible upgrade experience.

Shut Down and Power Off All Virtual Machines

If you plan to use virtual machines created under an earlier version of GSX Server, be sure they have been shut down completely before you remove the release you used to create them.

If any virtual machine is suspended, resume it in the earlier release, shut down the guest operating system, then power off the virtual machine.

Note: If you attempt to resume a virtual machine that was suspended under a different VMware product or a different version of GSX Server, a message appears, giving you the choice of discarding or keeping the file that stores the suspended state. To recover the suspended state, you must click **Keep**, then resume the virtual machine under the correct VMware product. If you click **Discard**, you can power on normally, but the suspended state is lost.

Make Sure All Disks Are in the Same Mode

If you have an existing virtual machine with one or more virtual disks, and all the disks use persistent or undoable mode, upgrading is straightforward.

If you have an existing virtual machine with one or more virtual disks, and all the disks use nonpersistent mode, you need to take a few special steps when you upgrade VMware Tools. For details, see www.vmware.com/info?id=44.

If you plan to use an existing virtual machine that has disks in undoable mode, commit or discard any changes to the virtual disks before you remove the release you used to create them.

Resume or power on the virtual machine in the earlier release, shut down the guest operating system, power off the virtual machine and either commit or discard changes to the disk in undoable mode when prompted.

If the disks are in persistent or nonpersistent mode, be sure the virtual machine is completely shut down. If it is suspended, resume it, shut down the guest operating system and power off the virtual machine.

If you have an existing virtual machine that has multiple virtual disks and the disks are in multiple modes, the simplest approach to upgrading is to convert all the disks to persistent mode.

Resume or power on the virtual machine in the earlier release, shut down the guest operating system, power off the virtual machine and either commit or discard changes to any undoable mode disks when prompted. Then open the Configuration Editor and change all disks to persistent mode. After you upgrade, you can use the snapshot feature to preserve the state of a virtual machine and return to that state at a later time. For more information on the snapshot feature, see [Taking Snapshots](#) in the *VMware GSX Server Virtual Machine Guide*.

If you need to preserve special functionality that requires disks in multiple modes, review the information at www.vmware.com/info?id=40 before you upgrade.

Back Up Virtual Machines

As a precaution, back up all the files in your virtual machine directories — including the `.vmdk` or `.disk`, `.vmx` or `.cfg` and `nvr`am files — for any existing virtual machines you plan to migrate to the new version of GSX Server. Depending on your upgrade path, you may not be able to run your virtual machines under both the new version of GSX Server and your previous version of GSX Server.

Virtual machines created under GSX Server 1 must have their virtual hardware updated before they can run under GSX Server 3. Once they are updated, they cannot be run under GSX Server 1.

You have a choice with virtual machines that you created under GSX Server 2 or updated to use the GSX Server 2 virtual hardware.

- You may update these virtual machines for full compatibility with GSX Server 3. In that case, the virtual machines can no longer be used under GSX Server 2.
- You may choose not to update the virtual hardware. In that case, you can run the virtual machines under both GSX Server 2 and GSX Server 3, but you do not have the benefits of the new virtual hardware provided by GSX Server 3. Other new features are not available. For example, you cannot take a snapshot or revert to the snapshot while the virtual machine is running; you must power off before taking or reverting to the snapshot.

Remove VMware GSX Server or VMware Workstation

If you have GSX Server installed on your host system, you must remove it before you install the new version. Also, see [When You Remove an Existing Version and Install the New Version on page 82](#).

If you have VMware Workstation installed on your host system, you must remove it before you install GSX Server. See the VMware Workstation product documentation for information on how to remove Workstation.

Make the Virtual Machine Accessible to Its Users

If the virtual machine is located on a different host or in a different directory on the GSX Server host, be sure to set permissions on the directory so that it is accessible to all users of the virtual machine. For more information on permissions, see [Securing Virtual Machines and the Host on page 106](#).

When You Remove an Existing Version and Install the New Version

There is a key precaution you should take when you remove an existing installation of GSX Server and install the new version.

Leave the Existing License in Place

The installation steps for your host may require that you run an uninstaller to remove a previous version of VMware GSX Server from your machine.

On a Windows host, the uninstaller asks whether you want to keep licenses in your registry. Do not remove the licenses. You can safely keep licenses for multiple versions of VMware products on the computer at the same time.

On a Linux host, the license remains in place. You do not need to take any special action. You may safely leave the license where it is.

Upgrading on a Windows Host

In most cases, upgrading GSX Server is a four-step process.

1. Uninstall the version now installed on your system. If you are uninstalling an older version of GSX Server 3, see [Uninstalling GSX Server on a Windows Host on page 73](#). If you are uninstalling version 1 or 2, see [Removing Version 1 or Removing Version 2](#), below.

Note: The uninstaller may offer to remove licenses from your registry. Do not remove the licenses.

2. If you are prompted, reboot your computer.
3. Install the latest version.
4. If you are prompted, reboot your computer.

Removing Version 2

To uninstall version 2, use the VMware GSX Server master installer. For details, see [Uninstalling GSX Server on a Windows Host on page 73](#). You need to keep your existing license in the Windows registry.

After you reboot, follow the instructions in [Installing VMware GSX Server on a Windows Host on page 40](#).

Removing Version 1

To uninstall GSX Server 1, use Add/Remove Programs in the Windows Control Panel. Be sure to uninstall GSX Server, the VMware Management Interface and the VMware Remote Console.

After you remove the three packages, reboot your host and follow the instructions in [Installing VMware GSX Server on a Windows Host on page 40](#).

Note: If you have VMware Workstation installed on your host system, you must remove it before you install GSX Server. See the VMware Workstation product documentation for information on how to remove Workstation.

Upgrading on a Linux Host

To upgrade from version 1 or 2 to version 3, you must have the full VMware GSX Server 3 product.

Upgrading Using the tar Installer

If you used the tar installer to install your current version of GSX Server, and you plan to use the tar installer for the new version, the only special step you need to take is to make sure the directory to which you plan to untar the tar archive does not contain any files from a previous GSX Server tar installation. You do not need to uninstall the older version. Just follow the installation instructions under [Installing VMware GSX Server on a Linux Host on page 50](#).

Upgrading Using the RPM Installer

If you used the RPM installer to install your current version of GSX Server, you need to uninstall the software before you upgrade to the new version. See [Uninstalling GSX Server on a Linux Host on page 78](#).

Using Virtual Machines Created with Version 2 under Version 3

The following sections describe how you can set up older virtual machines under VMware GSX Server 3 and how to upgrade the virtual hardware.

Creating Everything New from the Start

Set up a new virtual machine and install a guest operating system in the virtual machine as described in [Creating a New Virtual Machine](#) in the *VMware GSX Server Virtual Machine Guide*. Creating all new virtual machines is the easiest way to use the latest technology and enjoy the best possible virtual machine performance.

Using an Existing Virtual Machine without Upgrading the Virtual Hardware

Upgrade VMware Tools to the new version, following the instructions in [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide*. Do not remove the older version of VMware Tools before installing the new version.

A virtual machine set up in this way should run without problems. However, you do not have the benefits of certain new features, including better performance, improved networking, the ability to take a snapshot while the virtual machine is running and improved virtual disk formats. Also, the console interface changes to accommodate older virtual machine features. For more information, see [Connecting to Older GSX Server and ESX Server Systems and Older Virtual Machines](#) in the *VMware GSX Server Virtual Machine Guide*.

Note: The first time you power on the virtual machine under GSX Server 3, GSX Server updates the CMOS. As a result, your guest operating system may detect hardware changes and install new drivers for the new hardware even if you do not upgrade the virtual hardware. Similarly, if you switch back to GSX Server 2, your guest operating system may detect hardware changes and install the appropriate drivers. You should expect to see this behavior each time you switch from one version of VMware GSX Server to the other.

Using an Existing Virtual Machine and Upgrading the Virtual Hardware

If you use an existing virtual machine and upgrade the virtual hardware, you gain access to new features, but the process is one-way — you cannot reverse it.

Start by using an existing configuration file (.vmx) and virtual disk (.vmdk or .disk).

Upgrade VMware Tools to the new version, following the instructions in [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide*. Do not remove the older version of VMware Tools before installing the new version.

Upgrade the virtual hardware so you can take advantage of better performance, improved networking, support for taking a snapshot while the virtual machine is running and improved virtual disk formats. See [Upgrading Virtual Hardware in the Guest Operating System](#) on page 86.

Note: When you update the virtual hardware in a Windows XP or Windows Server 2003 virtual machine, the Microsoft product activation feature may require you to reactivate the guest operating system.

Upgrading Virtual Hardware in the Guest Operating System

Upgrading a virtual machine's virtual hardware gives it access to new features of GSX Server. Before you upgrade the virtual hardware, however, consider the following:

- **The virtual hardware upgrade is irreversible:** The process of upgrading the virtual hardware is irreversible and makes the disks attached to this virtual machine incompatible with VMware GSX Server 1 or 2. You should make backup copies of your virtual disks before starting the upgrade.
- **GSX Server 3 updates the CMOS:** If you are using a virtual machine created under VMware GSX Server 2, the first time you power on the virtual machine under VMware GSX Server 3, GSX Server updates the CMOS. As a result, your guest operating system may detect hardware changes and install new drivers for the new hardware even if you do not choose to upgrade the virtual hardware.
- **You must install VMware Tools:** You need to install the new version of VMware Tools. Do this before you upgrade the virtual hardware. For details, see [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide*.
- **An error may appear when upgrading from physical disk:** If you are upgrading a virtual machine that runs from a physical disk, rather than a virtual disk, you may see the following error message while VMware GSX Server is upgrading the virtual hardware: "Unable to upgrade <drivename>. One of the supplied parameters is invalid." You may safely click **OK** to continue the upgrade process.
- **Windows 95 and Windows 98 guests cannot load CD-ROM drivers at first:** The first time you run a VMware GSX Server 2 virtual machine under VMware GSX Server 3, the guest operating system discovers new hardware and attempts to install drivers for it before it loads the CD-ROM driver. As a result, it is unable to load drivers from the operating system installation CD. In many cases, the drivers

are already available in `C:\Windows`, `C:\Windows\System` or subdirectories under those two directories. However, a simpler approach is to skip any files that Windows does not find at this stage. Then, after the guest operating system has finished loading and is able to read from the CD-ROM, you can run the guest operating system's Add Hardware Wizard and allow it to detect new hardware and install the appropriate drivers.

Upgrading the Virtual Machine's Hardware

To upgrade the virtual hardware, choose **VM > Upgrade Virtual Hardware**. A message appears, warning that the upgrade process cannot be reversed. Click **Yes** to continue, then follow the directions.

When you upgrade the virtual hardware, you may then need to take several steps to be sure the new virtual hardware is recognized properly by the guest operating system. If your guest operating system is listed below, the instructions for that guest operating system provide examples of the steps you may need to take to perform these updates.

Windows 2000 Guest

The following steps provide examples of what you may see as your guest operating system recognizes the new virtual hardware. The specific steps may vary, depending on the configuration of the virtual machine.

1. Power on the virtual machine and let it update the CMOS.
2. Windows automatically installs the software for any devices it detects.
3. Install the new version of VMware Tools. For details, see [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide*.
4. Shut down the Windows guest and power off the virtual machine.
5. Choose **VM > Upgrade Virtual Hardware**.
6. A message cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding. To continue, click **Yes**.
7. A message describes what is about to happen. Click **OK** to continue.
8. Power on the virtual machine.
9. Windows detects the PCI SVGA adapter, then it detects the VMware SVGA II adapter. Click **Yes** to continue the installation.
10. A message asks you to insert a disk. Navigate to `C:\Program Files\VMware\drivers` to install the VMware SVGA II adapter.

11. If you have serial ports configured in the virtual machine, go to the Windows Device Manager and uninstall all the COM ports listed there.
12. Restart the virtual machine.
13. Windows detects the COM ports and installs them properly.

Windows NT 4.0 Guest

The following steps provide examples of what you may see as your guest operating system recognizes the new virtual hardware. The specific steps may vary, depending on the configuration of the virtual machine.

1. Power on the virtual machine and let it update the CMOS.
2. Windows displays a message about the video driver in the guest operating system. Click **OK**.
3. Install the new version of VMware Tools. For details, see [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide*.
4. Restart the Windows guest and confirm that it is operating correctly.
5. Shut down the Windows guest and power off the virtual machine.
6. Choose **VM > Upgrade Virtual Hardware**.
7. A message cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding. To continue, click **Yes**.
8. A message describes what is about to happen. Click **OK** to continue.
9. You can now power on the virtual machine and use the new configuration. Windows NT does not have a Plug and Play process, so no additional steps are required.

Windows XP Guest

The following steps provide examples of what you may see as your guest operating system recognizes the new virtual hardware. The specific steps may vary, depending on the configuration of the virtual machine.

1. Power on the virtual machine and let it update the CMOS.
2. Install the new version of VMware Tools. For details, see [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide*.
3. Shut down the Windows guest and power off the virtual machine.
4. Choose **VM > Upgrade Virtual Hardware**.
5. A message cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding. To continue, click **Yes**.

6. A message describes what is about to happen. Click **OK** to continue.
7. Power on the virtual machine.
8. Windows detects the VMware SVGA adapter. Select **Install the software automatically** and follow the on-screen instructions.
9. A message asks you to insert a disk. Navigate to `C:\Program Files\VMware\drivers` to install the VMware SVGA II adapter.
10. If you have serial ports configured in the virtual machine, go to the Windows Device Manager and uninstall all the COM ports listed there.
11. Restart the virtual machine.
12. Windows detects the COM ports and installs them properly.

Windows Me Guest

The following steps provide examples of what you may see as your guest operating system recognizes the new virtual hardware. The specific steps may vary, depending on the configuration of the virtual machine.

1. Power on the virtual machine and let it update the CMOS.
2. Plug and Play detects an Intel 82371 EB Power Management controller. Select **Automatic search** and click **Next**. Windows finds and installs the driver automatically.
3. Plug and Play detects an Intel 82443 BX Pentium II Processor to PCI bridge. Select **Automatic search** and click **Next**. Windows finds and installs the driver automatically.
4. Restart the guest operating system.
5. Plug and Play detects an Intel 82371 AB/EB PCI Bus Master IDE controller. Select **Automatic search** and click **Next**. Windows finds and install the driver automatically.
6. Install the new version of VMware Tools. For details, see [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide*.
7. Shut down the Windows guest and power off the virtual machine.
8. Choose **VM > Upgrade Virtual Hardware**.
9. A message cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding. To continue, click **Yes**.
10. A message describes what is about to happen. Click **OK** to continue.

11. Power on the virtual machine.
12. Windows detects the PCI Multimedia Audio device and installs the driver for the Creative AudioPCI.
13. Windows detects an AMD PCNet adapter. Select **Automatic search** and click **Next**. Windows automatically installs the driver for the adapter.
14. Click **Finish** to restart the virtual machine.
15. Windows detects a Creative game port device and installs the driver automatically.
16. Windows detects a game port joystick and installs the driver automatically.
17. Windows detects the PCI SVGA adapter, which it then identifies as the VMware SVGA II adapter and installs the driver automatically.
18. Click **Yes** to restart the virtual machine.
19. If you have serial ports configured in the virtual machine, go to the Windows Device Manager and uninstall all the COM ports listed there.
20. Restart the virtual machine.
21. Windows detects the COM ports and installs them properly.

Windows 98 Guest

The following steps provide examples of what you may see as your guest operating system recognizes the new virtual hardware. The specific steps may vary, depending on the configuration of the virtual machine.

1. Power on the virtual machine and let it update the CMOS.
2. Windows detects a PCI to ISA bridge. Go to `C:\Windows\System` and let Windows select the necessary driver.
3. Windows detects an Intel 82371EB Power Management Controller. Go to `C:\Windows\System` and let Windows select the necessary file.
4. Windows detects `lpt.vxd`. Go to `C:\Windows\System` and let Windows select the necessary file.
5. Windows detects an Intel 82443BX Pentium Processor to PCI bridge. Go to `C:\Windows\System` and let Windows select the necessary file.
6. Windows detects an Intel 82371AB/EB PCI Bus Master IDE controller. Go to `C:\Windows\System` and let Windows select the necessary file.
7. Windows asks for the file `uhcd.sys`. Enter the location `C:\Windows\System32\drivers`, then click **OK**.

8. Windows detects an Intel 82371AB/EB PCI to USB Universal host controller. Go to `C:\Windows\System` and let Windows select the necessary file.
9. Windows detects an AMD PCNET Family Ethernet Adapter. Go to `C:\Windows\System` and let Windows select the necessary file.
10. Windows asks for the file `inetmib1.dll`. Enter the location `C:\Windows`, then click **OK**.
11. Windows asks for the file `locproxy.exe`. Enter the location `C:\Windows\System`, then click **OK**.
12. Windows asks for the file `ndishlp.sys`. Enter the location `C:\Windows`, then click **OK**.
13. Windows asks for the file `wsock.vxd`. Enter the location `C:\Windows\System`, then click **OK**.
14. When you finish installing the AMD Family Ethernet Adapter, restart Windows 98.
15. Plug and Play detects multiple devices and restarts Windows 98.
16. After the virtual machine restarts, install the new version of VMware Tools. For details, see [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide*.
17. Shut down the Windows guest and power off the virtual machine.
18. Choose **VM > Upgrade Virtual Hardware**.
19. A message cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding. To continue, click **Yes**.
20. A message describes what is about to happen. Click **OK** to continue.
21. Power on the virtual machine. When Windows boots, it detects the PCI SVGA adapter. Later, it detects the VMware SVGA II adapter and installs the driver for it automatically.
22. Windows detects PCI Multimedia Audio and offers to install a driver for it. Click **Cancel**.
23. Windows detects an AMD PCNET Family Ethernet adapter. Click **Next**.
24. Select **Search for the best driver** and click **Next**.
25. Select **Specify a location**, enter `C:\Windows\System` and click **Next**.
26. Select **The updated driver (Recommended) AMD PCNET Family Ethernet Adapter (PCI-ISA)**. Click **Next**.
27. Windows finds the `.inf` file for the adapter. Click **Next**.

28. Windows asks for the file `dhcpcsvc.dll`. Enter the location `C:\Windows\System`, then click **OK**.
29. Windows asks for the file `inetmib1.dll`. Enter the location `C:\Windows`, then click **OK**.
30. Windows asks for the file `locproxy.exe`. Enter the location `C:\Windows\System`, then click **OK**.
31. Windows asks for the file `ndishlp.sys`. Enter the location `C:\Windows`, then click **OK**.
32. Windows asks for the file `wshtcp.vxd`. Enter the location `C:\Windows\System`, then click **OK**.
33. A dialog box indicates that Windows has finished installing the software. Click **Finish**.
34. To install the sound adapter, follow the directions in [Installing Sound Drivers in Windows 9x and Windows NT Guest Operating Systems](#) in the *VMware GSX Server Virtual Machine Guide*.
35. If you have serial ports configured in the virtual machine, go to the Windows Device Manager and uninstall all the COM ports listed there.
36. Restart the virtual machine.
37. Windows detects the COM ports and installs them properly.

Windows 95 Guest

The following steps provide examples of what you may see as your guest operating system recognizes the new virtual hardware. The specific steps may vary, depending on the configuration of the virtual machine.

1. Power on the virtual machine and let it update the CMOS.
2. Windows detects new devices and automatically installs the drivers. Restart the guest operating system after this process is complete.
3. When Windows restarts, it detects more new devices.
4. Windows asks for the file `lpt.vxd`. Enter the location `C:\Windows\System`, then click **OK**.
5. Windows detects a PCI standard host bridge and other devices. Click **OK** to dismiss these messages. You do not need to install these drivers.
6. Click **Finish**.

7. Install the new version of VMware Tools. For details, see [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide*.
8. Shut down the Windows guest and power off the virtual machine.
9. Choose **VM > Upgrade Virtual Hardware**.
10. A message cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding. To continue, click **Yes**.
11. A message describes what is about to happen. Click **OK** to continue.
12. Windows detects a PCI Multimedia Audio device. Click **Cancel**.
13. Windows detects a PCI Ethernet adapter, then the AMD Ethernet adapter. Windows automatically installs the driver.
14. To install the sound adapter, follow the directions in [Installing Sound Drivers in Windows 9x and Windows NT Guest Operating Systems](#) in the *VMware GSX Server Virtual Machine Guide*.
15. If you have serial ports configured in the virtual machine, go to the Windows Device Manager and uninstall all the COM ports listed there.
16. Restart the virtual machine.
17. Windows detects the COM ports and installs them properly.

Red Hat Linux or SuSE Linux Guest

The following steps provide examples of what you may see as your guest operating system recognizes the new virtual hardware. The specific steps may vary, depending on the configuration of the virtual machine.

1. Power on the virtual machine and let it update the CMOS.
2. When Kudzu appears, follow the instructions to detect new hardware and install the proper drivers.
3. Shut down the Linux guest and power off the virtual machine.
4. Choose **VM > Upgrade Virtual Hardware**.
5. A message cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding. To continue, click **Yes**.
6. A message describes what is about to happen. Click **OK** to continue.
7. Power on the virtual machine.
8. When Kudzu runs, it detects an Ensoniq:ES1371 [AudioPCI-97] sound device.
9. Click **Configure**.

Mandrake Linux Guest

The following steps provide examples of what you may see as your guest operating system recognizes the new virtual hardware. The specific steps may vary, depending on the configuration of the virtual machine.

1. Power on the virtual machine and let it update the CMOS.
2. When Kudzu appears, follow the instructions to detect new hardware and install the proper drivers.
3. Shut down the Linux guest and power off the virtual machine.
4. Choose **VM > Upgrade Virtual Hardware**.
5. A dialog box cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding. To continue, click **Yes**.
6. A message describes what is about to happen. Click **OK** to continue.
7. Power on the virtual machine.
8. When Kudzu runs, it detects an Ensoniq:ES1371 [AudioPCI-97] sound device.
9. Click **Configure**.

Note: When using Kudzu, do not migrate the existing network configuration. If you try to do so, you see a blank screen. Instead, click **No** when asked if you want to migrate the existing network configuration.

Using Virtual Machines Created with Version 1 under Version 3

If you use an existing VMware GSX Server 1 virtual machine under VMware GSX Server 3, the virtual hardware is upgraded automatically. The upgrade gives you access to new features, but the process is one-way — you cannot reverse it.

Start by using an existing configuration file (.vmx or .cfg) and virtual disk (.disk or .vmdk).

The first time you power on the virtual machine under GSX Server 3, a dialog box appears, offering the choice of upgrading the virtual hardware or powering off. If you want to make a backup copy of the virtual machine before upgrading the virtual hardware, power off and make the backup. Otherwise, allow VMware GSX Server to upgrade the virtual hardware. See [Upgrading Virtual Hardware in the Guest Operating System](#) below.

Note: If you are upgrading a virtual machine that runs from a physical disk, rather than a virtual disk, you may see the following error message while VMware GSX Server is upgrading the virtual hardware: "Unable to upgrade <drivename>. One of the supplied parameters is invalid." You may safely ignore the error message, then click **OK** to continue the upgrade process.

Upgrade VMware Tools to the new version following the instructions for your guest operating system in [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide*. You should not remove the older version of VMware Tools before installing the new version.

Upgrading Virtual Hardware in the Guest Operating System

After upgrading the virtual hardware, you may need to take several steps to be sure the new virtual hardware is recognized properly by the guest operating system. If you are using a Windows 95, Windows 98 or Windows Me virtual machine created under VMware GSX Server 1, take the steps listed under the name of your guest operating system.

If you are using other guest operating systems, you do not need to take these special steps. Plug and Play should recognize the new virtual hardware and install any needed drivers smoothly.

In any case, you should verify the guest operating system selection in the virtual machine settings editor. See [Check Guest Operating System Selection on page 98](#).

Windows Me Guest

The following steps provide examples of what you may see as your guest operating system recognizes the new virtual hardware. The specific steps may vary, depending on the configuration of the virtual machine.

1. Power on the virtual machine.
2. Allow GSX Server to upgrade the virtual hardware.
3. Click **OK** to dismiss the message “A legacy SVGA driver has been detected.”
4. Several Plug and Play messages appear. You can safely ignore them.
5. Log on to Windows Me. More Plug and Play messages appear. One refers to the VMware SVGA driver. You can ignore these messages until you are prompted to restart the guest operating system.

Click **Yes** to restart your virtual machine.

6. Log on to Windows Me. The SVGA driver is not working properly.
7. From the Windows **Start** menu, choose **Settings > Control Panel > System > Device Manager > Display Adapters**.

Manually remove the two SVGA drivers.

8. Restart the Windows guest.
A VMware SVGA II adapter is detected and Windows installs it.
Windows notifies you to restart your computer.
Click **Yes**.
9. The SVGA driver should now be working correctly.
10. Install the new version of VMware Tools. See [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide* for details.

Windows 98 Guest

The following steps provide examples of what you may see as your guest operating system recognizes the new virtual hardware. The specific steps may vary, depending on the configuration of the virtual machine.

1. Power on the virtual machine.
2. Allow GSX Server to rename the virtual disk with the `.vmdk` extension.
3. Allow GSX Server to upgrade the virtual hardware.

4. Click **OK** to dismiss the message "A legacy SVGA driver has been detected."
5. Log on to Windows 98. You see a number of Plug and Play messages. You may need to insert your Windows 98 installation CD.
6. Windows asks for the `Pcimp.pci` file. Enter `C:\Windows\System` as the location.
7. Windows detects an Intel 82371EB PCI to ISA bridge (ISA mode). Go to `C:\Windows\System` and let Windows select the driver or select automatic detection.
8. Windows detects an Intel 82371ES Power Management Controller. Go to `C:\Windows\System` and let Windows select the driver or select automatic detection.
9. Windows detects a PS/2 compatible mouse port. Go to `C:\Windows\System` and let Windows select the driver.
10. Windows detects the COM port. Go to `C:\Windows\System` and let Windows select the driver.
11. Windows detects a printer port. Browse for the `Lpt.vxd` file.
12. Windows detects an Intel 82443Bx Pentium(r) II Processor to PCI bridge (with GART support). Go to `C:\Windows\System` and let Windows select the driver.
13. Windows detects a Standard Dual PCI IDE Controller. Go to `C:\Windows\System` and let Windows select the driver.
14. Windows detects an Intel 82371AB/EB PCI to USB Universal Host Controller. Go to `C:\Windows\System` and let Windows select the driver.
15. Windows detects an AMD PCNET Family Ethernet Adapter (PCI-ISA). Go to `C:\Windows\System` and let Windows select the driver.
16. Windows asks for the location of the `serialui.dll` driver. Enter `C:\Windows\System` as the location.
17. Restart the Windows guest.
18. The SVGA driver should now be working correctly.
19. Install the new version of VMware Tools. See [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide* for details.

Windows 95 Guest

The following steps provide examples of what you may see as your guest operating system recognizes the new virtual hardware. The specific steps may vary, depending on the configuration of the virtual machine.

1. Power on the virtual machine.
2. Allow GSX Server to upgrade the virtual hardware.
3. Click **OK** to dismiss the message “A legacy SVGA driver has been detected.”
4. Log on to Windows 95.

You see a number of Plug and Play messages. Click **Cancel** for those listing the Standard host CPU bridge, PCI bridge and PCI Universal bus devices.

5. The SVGA driver is not working properly.
6. From the Windows **Start** menu, choose **Settings > Control Panel > System > Device Manager > Display Adapters**. Manually remove the SVGA driver.
7. Restart the Windows guest.
8. Again, you see a number of Plug and Play messages. Click **Cancel** for those listing the Standard host CPU bridge, PCI bridge and PCI Universal bus devices.
9. Windows detects and installs the VMware SVGA II adapter.
10. Restart Windows 95.
11. Once again, you see a number of Plug and Play messages. Again, click **Cancel** for those listing the Standard host CPU bridge, PCI bridge and PCI Universal bus devices.
12. The SVGA driver should now be working correctly.
13. Install the new version of VMware Tools. See [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide* for details.

Check Guest Operating System Selection

Some operating systems, such as Windows Server 2003 and Windows 2000, have multiple versions. Verify your guest operating system is set to the specific version of the operating system installed in the virtual machine. Check the setting in the virtual machine settings editor (choose **VM > Settings > Options**).

4

CHAPTER

Managing Virtual Machines and the VMware GSX Server Host

The following sections describe how to manage your virtual machines and the GSX Server host:

- [Remotely Managing Virtual Machines on page 101](#)
- [Changing the Port Number for VMware Virtual Machine Console Connections on page 101](#)
- [Downloading the VMware Virtual Machine Console on page 104](#)
- [Securing Virtual Machines and the Host on page 106](#)
- [Understanding Permissions and Virtual Machines on page 106](#)
- [Authenticating Users and Running Virtual Machines on a GSX Server for Windows Host on page 108](#)
- [Authenticating Users and Running Virtual Machines on a GSX Server for Linux Host on page 111](#)
- [Checking Permissions in the VMware Management Interface on page 112](#)
- [Securing Your Remote Sessions on page 112](#)
- [Identifying a Virtual Machine by Its UUID on page 115](#)

- [Logging GSX Server Events on Windows on page 117](#)
- [Backing Up Virtual Machines on page 119](#)
 - [Using a Backup Agent in the Virtual Machine on page 119](#)
 - [Using a Backup Agent Running on the Host Operating System on page 119](#)
 - [Backing Up the GSX Server Host on page 120](#)
 - [Considerations for Backing Up Virtual Machines on page 120](#)
- [Using the VMware Management Interface on page 121](#)
 - [Setting the Session Length for the VMware Management Interface on page 122](#)
 - [Logging In to the VMware Management Interface on page 122](#)
 - [Using the Status Monitor on page 124](#)
 - [Configuring a Virtual Machine on page 130](#)
 - [The Apache Server and the VMware Management Interface on page 141](#)
 - [Logging Out of the VMware Management Interface on page 141](#)
- [Deleting Virtual Machines on page 142](#)
 - [Deleting a Virtual Machine Using the VMware Virtual Machine Console on page 142](#)
 - [Deleting a Virtual Machine Using the VMware Management Interface on page 142](#)
- [Configuring the GSX Server Host on page 143](#)
 - [Configuring GSX Server from the Management Interface on page 143](#)
 - [Setting User Preferences for the VMware GSX Server Host on page 149](#)
 - [Setting Global Preferences for VMware GSX Server on page 154](#)
 - [Setting a MIME Type to Launch the VMware Virtual Machine Console on page 157](#)

Remotely Managing Virtual Machines

One of the primary strengths of GSX Server is that it allows you to manage your virtual machines remotely — that is, from any machine that can connect to your GSX Server host. You are not restricted to interacting with your virtual machines only on the host on which they are stored.

Remote management has many components and levels. For a high level view of your GSX Server host, use the VMware Management Interface, a Web-based tool for managing your virtual machines and the server host. For more information about the management interface, see [Using the VMware Management Interface on page 121](#).

If you need to interact with a virtual machine directly from a remote location — for example, if you need to maintain a database stored in a virtual machine — use the VMware Virtual Machine Console. The console displays your virtual machine in a window, and you interact with the virtual machine in this window as you would interact with a physical computer. For more information about consoles, see [Running Virtual Machines](#) in the *VMware GSX Server Virtual Machine Guide*.

For a more automated way to remotely manage virtual machines and the GSX Server host, use the VMware Scripting APIs. If you are connecting to a GSX Server host from a Windows remote machine, you can use the VmCOM and VmPerl Scripting APIs. If you are connecting to a GSX Server host from a Linux remote machine, you can use the VmPerl Scripting API. For more information, visit the VMware Web site at www.vmware.com/support/developer.

Another automated way to manage virtual machines is to use the `vmware-cmd` utility. For more information, visit the VMware Web site at www.vmware.com/support/developer.

Finally, you can use third party tools to remotely manage your virtual machines. You can use applications like VNC Viewer, Windows Terminal Services or Windows XP Remote Desktop. To view a virtual machine with VNC Viewer, you must modify the virtual machine's configuration manually.

Changing the Port Number for VMware Virtual Machine Console Connections

By default, the VMware Virtual Machine Console connects to virtual machines via port 902. If this port assignment poses a conflict for your site — for example, if you use the `idea farm-chat` program — you can change the port number the console uses accordingly.

Changing the port number involves manually adding a variable to certain preference files. The steps you need to take vary depending upon the server host operating system, the host on which the console is running and whether you are making this change to GSX Server itself (by assigning the new port number to a variable called `authd.port`) or to the console (by assigning the new port number to a variable called `authd.client.port`).

The `authd.port` setting is different from the `authd.client.port` setting. The `authd.port` variable tells GSX Server (the server side) which port to listen on for console connections from remote hosts or clients. The `authd.client.port` variable tells the console (the client side) the port with which to connect. Thus, if you set only `authd.port` to a different port number, such as 9902, and you try to connect to a virtual machine on that host with a console on a remote host or client, the console still tries to connect to port 902. Keep in mind that you can substitute this new port number manually when you connect with a console. In the Connect to VMware Server dialog box, in the **Host name** field, enter the port number along with the name of the GSX Server host name and configuration file path, like this:

```
<server name>:<port> <config file>
```

Depending upon your site's needs or configuration (for example, if you have multiple GSX Server hosts and they use different ports), this might be acceptable. However, setting `authd.client.port` to the same port number you use for `authd.port` allows for seamless integration between the server and the console. It also lets you avoid manually entering the port number every time you connect to the server with a console.

Changing the Port Number on a Windows Host

To change the port number on the GSX Server for Windows host, you must modify `config.ini` in `C:\Documents and Settings\All Users\Application Data\VMware\VMware GSX Server`. In this file, set the new port number to the `authd.port` variable. All consoles connecting to virtual machines on this host must use this port number.

To change the port number that is used by the console installed on a Windows host, you must create a file called `config.ini` and place it in `C:\Documents and Settings\All Users\Application Data\VMware\VMware Virtual Machine Console`. In this file, set the new port number to the `authd.client.port` variable. All consoles on this machine connecting to virtual machines on the GSX Server host use this port number. The GSX Server host must have this port number set to the `authd.port` variable in its `config.ini` file (Windows host) or `vmware-authd` file (Linux host).

To change the port number for a specific user who is using the console installed on a Windows host, you need to set the new port number to the `authd.client.port` variable in the `preferences.ini` file located in `C:\Documents and Settings\<user>\Application Data\VMware`. This port number is used only when this user is logged in and using a console to connect to a virtual machine on the GSX Server host. The GSX Server host must have this port number set to the `authd.port` variable in its `config.ini` file (Windows host) or `vmware-authd` file (Linux host).

Changing the Port Number on a Linux Host

To change the port number on the GSX Server for Linux host, you first need to determine whether your host is configured to use `xinetd` or `inetd`. If your host is configured to use `xinetd`, change the port number in the `port = 902` line in the `/etc/xinetd/vmware-authd` file. If your host is configured to use `inetd`, change the port number in the `902 ... vmware-authd` line in `/etc/inetd.conf`. All consoles connecting to virtual machines on this host must use this port number.

To change the port number that is used by the console installed on a Linux host, you must set the new port number to the `authd.client.port` variable in either `/etc/vmware-console/config` or `/usr/lib/vmware-console/config`.

All consoles on this machine connecting to virtual machines on the GSX Server host use this port number. The GSX Server host must have this port number set to the `authd.port` variable in its `config.ini` file (Windows host) or `vmware-authd` file (Linux host).

Note: If the port numbers specified in these files are different, the port number specified in `/etc/vmware-console/config` takes precedence.

To change the port number for a specific user who is using the console installed on a Linux host, you need to set the new port number to the `authd.client.port` variable in `~/ .vmware/preferences`. This port number is used only when this user is logged in and using a console to connect to a virtual machine on the GSX Server host. The GSX Server host must have this port number set to the `authd.port` variable in its `config.ini` file (Windows host) or `vmware-authd` file (Linux host). When this user is logged in, the port number specified in `~/ .vmware/preferences` supersedes the port number specified in `/etc/vmware-console/config` or `/usr/lib/vmware-console/config`.

Substituting a Port Number with the VMware Scripting APIs

With the VMware Scripting APIs, you can supply a different port number when you create a new virtual machine object. This port number must match the port number set on the GSX Server host, which is set by the `authd.port` variable in the `config.ini` file (Windows host) or `vmware-authd` file (Linux host).

If you specify 0 as the port number, the console connects with the port number specified by `authd.client.port` instead. If `authd.client.port` is not specified, the console connects with the default port 902.

For more information about the VMware Scripting APIs, visit the VMware Web site at www.vmware.com/support/developer.

Downloading the VMware Virtual Machine Console

You can download installation packages for the VMware Virtual Machine Console from the VMware Management Interface. Packages are available for Linux and Windows hosts; download the package appropriate to the host machine on which the console is to be installed.

Downloading the console and installing it allows you to quickly launch the console from the management interface and manage virtual machines.

Downloading the installer from the Status Monitor page allows you to quickly download the console you need without logging out of the management interface.

Caution: Do not install a console from a client installer package onto the GSX Server 3 host. Do not download and install a console from an older version of GSX Server or ESX Server onto any client.

To download and install a console package from the Login or Status Monitor page, complete the following steps.

1. Connect to the GSX Server host with the VMware Management Interface. For information on connecting to the management interface, see [Logging In to the VMware Management Interface on page 122](#).
2. On the Status Monitor page, download the installer by clicking the link for the package appropriate to the operating system on which the console is to be installed.

On the Login page, select the installer appropriate to the operating system of the computer where you are installing the console, then click **Download**.

If you are installing the console on a Linux host, you can further choose between tar and RPM installation packages.

3. Run the installation package.

To install the console on a Windows system, see [Installing the VMware Virtual Machine Console on a Windows Host on page 64](#).

To install the console on a Linux system, see [Installing the VMware Virtual Machine Console on a Linux Host on page 67](#).

Customizing the Download Menu

You can customize the download menu on the Login page to suit your users' needs. For example, if your site uses the VMware Scripting APIs, you can add the API installers to the download menu. Client packages containing the VMware Virtual Machine Console and the VMware Scripting APIs are available on your GSX Server CD-ROM or in the packages you downloaded from the VMware Web site. The client packages are:

- `VMware-gsx-server-win32-client-<xxxx>.zip`
- `VMware-gsx-server-linux-client-<xxxx>.zip`

You can expand these archives and place the API installer files in a readily available area, then modify the download menu on the Login page to point to them.

You can add more files to the download menu, hide items already listed and even hide the link or the menu itself. Click **Help** on the Login page and follow the instructions there.

Note: On a Windows host with the VMware Management Interface installed, you can find the installers for the console and scripting APIs in `C:\Program Files\VMware\VMware Management Interface\htdocs\vmware\bin`. This folder contains:

- `VMware-console-<xxxx>.exe` — the installer for the VMware Virtual Machine Console to run on Windows clients.
- `VMware-console-<xxxx>.i386.rpm` — the RPM installer for the VMware Virtual Machine Console to run on Linux clients.
- `VMware-console-<xxxx>.tar.gz` — the tar installer for the VMware Virtual Machine Console to run on Linux clients.
- `VMware-VmCOMAPI-<xxxx>.exe` — the installer for the VmCOM API for Windows hosts only.
- `VMware-VmPERLAPI-<xxxx>.exe` — the installer for the VmPerl API for Windows hosts.

Securing Virtual Machines and the Host

This section describes how you can set permissions and implement security features for your virtual machines and the server host.

The VMware Knowledge Base has an article about best practices you can use to improve security for the GSX Server host and virtual machines. For information, see www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=1042.

Understanding Permissions and Virtual Machines

Access to a virtual machine is based on the permissions you, as a user, are granted to the virtual machine's configuration file (.vmx). Different permissions let you access virtual machines in different ways. These ways include:

- Browsing virtual machines.
- Interacting with virtual machines.
- Configuring virtual machines.
- Administering virtual machines and the host.

If the virtual machine is on a Windows host, permissions on more virtual machine files may be needed, depending upon the user account the virtual machine uses while running. For information, see [Authenticating Users and Running Virtual Machines on a GSX Server for Windows Host on page 108](#).

Browsing a Virtual Machine

Browsing a virtual machine lets you connect to it with a console, but you can see only the virtual machine's power state. The virtual machine display is blank, even if the virtual machine is running. You cannot interact with the virtual machine at all.

To browse a virtual machine, you need **Read** permission for the virtual machine's configuration file on a Windows host, or read (r) permission on a Linux host.

Interacting with a Virtual Machine

Interacting with a virtual machine lets you change its power state (power it on or off, suspend or resume it) and connect or disconnect removable devices. You cannot change the virtual machine's configuration. Among other restrictions, this means you cannot add or remove virtual hardware.

Your user name appears in the VMware Management Interface and in the Connected Users dialog box, which you access in the VMware Virtual Machine Console by choosing **VM > Connected Users**.

To interact with a virtual machine, you must have **Read & Execute** permission for the virtual machine's configuration file on a Windows host, or read and execute (`r` and `x`) permissions on a Linux host.

Configuring a Virtual Machine

Configuring a virtual machine lets you add and remove virtual hardware to and from the virtual machine.

To configure a virtual machine, you must have **Read** and **Write** permissions for the virtual machine's configuration file and virtual machine resources (such as a physical disk or certain devices) on a Windows host, or read and write (`r` and `w`) permissions on a Linux host.

Administering Virtual Machines and the GSX Server Host

An administrator or root user can configure the GSX Server host and any virtual machines on the host. For example, you can enable SSL for console connections or change the amount of host memory allocated for all virtual machines.

To administer a virtual machine on a Windows host, your user account must be a member of the host's Administrators group. On a Linux host, you should have root access to the directories containing virtual machine files.

Alternatively, your user account can have **Read & Execute** and **Write** permissions on a Windows host, or read, write and execute (`r`, `w` and `x`) permissions on a Linux host to a particular virtual machine.

If You Have No Permissions

If you have no permissions for the virtual machine's configuration file, then you cannot connect to the virtual machine at all. On a Windows host, if a permission is both allowed and denied, the denial takes precedence. If permissions are neither allowed nor denied, then you are considered to have no permissions.

Only You Can See a Virtual Machines You Create

When you create a new virtual machine, the virtual machine by default is private; other users cannot see or use the virtual machine. If you want all users to be able to use the virtual machine, follow the custom path when you create the virtual machine.

Otherwise, you can change the private setting in the virtual machine settings editor.

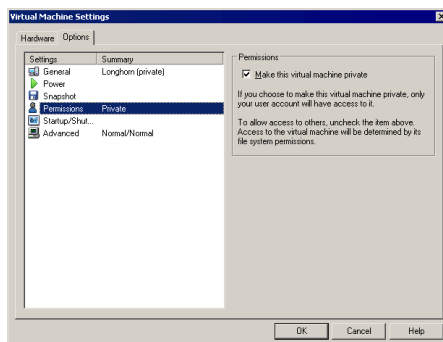
When a virtual machine is private, it appears in the inventory of the console of the user who created it. The virtual machine does not appear in the inventory of consoles for other users connected to the host. The virtual machine appears in the VMware Management Interface only when you are logged in with the account that created the virtual machine.

Other users cannot browse to the virtual machine and add it to the inventory.

If the virtual machine is made private after it has been created, it disappears from other users' inventories.

To specify whether a virtual machine is private after it has been created, complete the following steps.

1. Select the virtual machine in a console and choose **VM > Settings**. The virtual machine settings editor appears.
2. Click the **Options** tab, then click **Permissions**.



3. To make the virtual machine private, check **Make this virtual machine private**. To allow all users to see and use this virtual machine, clear the check box.
4. Click **OK** to save your settings and close the virtual machine settings editor.

Authenticating Users and Running Virtual Machines on a GSX Server for Windows Host

Every time you connect to a GSX Server for Windows host with the VMware Virtual Machine Console or VMware Management Interface, the VMware Authorization Service requests a username and password, then authenticates only valid users.

Once you are authenticated, the console starts or the management interface's Status Monitor page appears. What you can now do with a virtual machine is based on your permissions. See [Understanding Permissions and Virtual Machines on page 106](#).

Each virtual machine runs as one of the following three user accounts:

- **The user who powers on the virtual machine** — the virtual machine runs as the account of the user who powered on the virtual machine until the virtual machine is powered off. Other users can connect to the virtual machine but it still runs as the user who powered on the virtual machine.

- **The local system account** — the virtual machine runs as the local system account (Administrator). You can enable this option only if you are logged in to the host operating system as an Administrator.
- **A specific user account** — the virtual machine runs as the user account specified in the New Virtual Machine Wizard or the virtual machine settings editor. This account must be able to access the GSX Server host.

The user account is specified when you create the virtual machine and you can change it in the virtual machine settings editor.

Understanding Permissions and User Accounts

If the virtual machine is configured to run as the user who powers it on, the user must have **Read** and **Write** permissions to the virtual machine files, such as the configuration file, virtual disk files and snapshot files. The user account must be an administrator account if the virtual machine needs to access devices like physical disks, USB controllers and generic SCSI devices.

An easy way to allow this user to access a virtual machine is to set the permissions for the directory containing the virtual machine files and let the user inherit the rights for that directory.

If another user connects to this virtual machine while it is running, that user only needs permissions for the configuration file.

For virtual machines configured to run as a specific user account or run as the local system user, any user connecting to the virtual machine needs permissions for the configuration file only.

An easy way to allow these users to access the virtual machine is to grant **Read** and **Write** permissions to all the files in the virtual machine's directory except for the configuration file. Grant **Read & Execute** permission to the configuration file and disallow the inheritance of permissions on the file.

Changing the User Account

You can change the user account for a virtual machine by choosing **VM > Settings > Options > Startup/Shutdown** and changing the user account information there.

If the virtual machine is configured to run as the user account who powers it on, you need to make sure the virtual machine is in a location that is accessible to that user. If you need to locate the virtual machines in a different area, or on another system on the network, make sure the user has access to the virtual machine resources (such as virtual disks, physical disks, devices and snapshot files).

To change the location where virtual machines are created, see [Specifying Where Virtual Machines Are Created on page 154](#).

Permissions and Virtual Machine Devices

If you intend to configure a virtual machine to use a physical disk or generic SCSI device, the user account that the virtual machine runs as must be a member of the Administrators group.

Configuring Permissions to Access a Virtual Machine

The system administrator (that is, the administrator responsible for setting up the host running GSX Server, not necessarily the Windows Administrator login) can set the access permissions on the configuration file using the following procedure. In general, you would want your GSX Server users to have **Read** permission to virtual machine configuration files; you can add any specific users that should have **Read & Execute** and **Write** permissions.

1. Locate the configuration file on the host system. Right-click the configuration file and select **Properties**. The Properties dialog box appears.
2. Click the **Security** tab.

Note: If the virtual machine is stored on a Windows XP client system, and is configured to use Workgroup mode, the Security tab is hidden by default. To show the tab, on the Windows XP system, choose **Start > Control Panel > Folder Options**, click **Advanced** and clear the **Simple File Sharing** check box.

3. In the Properties dialog box, select each user or group and select the appropriate permission, typically **Read**.

If you want to limit access to the virtual machine, clear the **Allow inheritable permissions from parent to propagate to this object** check box.

4. To specify that a user or group that should not have access to the configuration file, either click **Remove** or check all permissions in the **Deny** column to deny all permissions to that user or group.
5. To add more users or groups, click **Add**. The Select Users, Computers and Groups dialog box appears. In the dialog box, select the groups or users that you want to access the virtual machine, then click **Add**. After you finish adding the users or groups, click **OK**. The users and groups are added with default **Read** and **Write** permissions. In the Properties dialog box, change the type of access for the user or group to the configuration file; choose either **Read** or **Read & Execute** and **Write**. Click **OK** to set the permissions to the configuration file.

Authenticating Users and Running Virtual Machines on a GSX Server for Linux Host

GSX Server for Linux uses Pluggable Authentication Modules (PAM) for user authentication in the VMware Virtual Machine Console and the VMware Management Interface. The default installation of GSX Server uses standard Linux `/etc/passwd` authentication, but can be configured to use LDAP, NIS, Kerberos or another distributed authentication mechanism.

Every time you connect to the GSX Server host with the VMware Virtual Machine Console or VMware Management Interface, the `inetd` or `xinetd` process runs an instance of the VMware authentication daemon (`vmware-authd`). The `vmware-authd` process requests a username and password, then hands them off to PAM, which performs the authentication.

Once you are authenticated, the console starts or the management interface's Status Monitor page appears. What you can now do with the virtual machines is based on your permissions. See [Understanding Permissions and Virtual Machines on page 106](#).

The `vmware-authd` process starts a virtual machine process as the owner of the configuration file, not as the user connecting to the virtual machine. However, the user is still restricted by his or her permissions on the configuration file.

Note: Even if you have full permissions on a configuration file, but you do not have execute permission to the directory in which the configuration file resides or any of its parent directories, then you cannot connect to the virtual machine with a VMware Virtual Machine Console or a VMware Scripting API. Furthermore, you cannot see the virtual machine in the VMware Management Interface or in the VMware Virtual Machine Console. Nor can you delete any files in the virtual machine's directory.

Note: Virtual machines and their resources (such as virtual disks, physical disks, devices and snapshot files) should be located in areas accessible to their users.

If a `vmware` process is not running for this configuration file, `vmware-authd` checks to see if this virtual machine is in the inventory. If the virtual machine is in the inventory, `vmware-authd` becomes the owner of the configuration file (not necessarily the user that is currently authenticated) and starts the console with this configuration file as an argument (for example, `vmware /<path_to_config>/<configfile>.vmx`).

The `vmware-authd` process exits as soon as a connection is established to a `vmware` process and at least one user has connected. Each `vmware` process shuts down automatically after the last user disconnects.

Default Permissions

When you create a virtual machine with GSX Server on a Linux host, its configuration file is assigned the following default permissions, based on the user accessing it:

- Read, execute and write (7) — for the user who created the configuration file (the owner)
- Read and execute (5) — for the primary group to which the owner belongs
- Read (4) — for users other than the owner or a member of the owner's group

When you first install the GSX Server software and run the configuration program `vmware-config.pl`, you can set these permissions for any existing virtual machine configuration files. If you plan to use a virtual machine and its configuration file you created in other VMware products with GSX Server, you must open the configuration file (choose **File > Open Virtual Machine**) in order to connect to the virtual machine from the VMware Virtual Machine Console or the VMware Management Interface, then set the default permissions as above.

Creating Virtual Machines on NFS Shares

If the virtual machine is located on an NFS share, make sure the root user has access to the location of the virtual machine files. Otherwise, you may encounter problems configuring the virtual machine.

If you create a virtual machine on an NFS share to which the root user has no access, certain operations do not work when the virtual machine is not running. For example, you cannot revert to a snapshot, add or remove devices to or from the virtual machine, or otherwise change the virtual machine's configuration.

Checking Permissions in the VMware Management Interface

The VMware Management Interface lists the permissions you have for each configuration file on the host machine to which you are connected. The permissions appear on the Users and Events page for each virtual machine. For more information, see [Viewing a List of Connected Users on page 139](#).

Only virtual machines for which you have read access are visible to you in the VMware Management Interface.

Securing Your Remote Sessions

The username, password and network packets sent to the GSX Server host over a network connection when using the VMware Virtual Machine Console or the VMware Management Interface are encrypted in GSX Server by default. As the Administrator user (Windows hosts) or root user (Linux hosts), you can disable Secure Sockets Layer (SSL) if you do not want to encrypt these sessions.

With SSL enabled, GSX Server creates security certificates and stores them on your host. However, the certificates used to secure your VMware Management Interface sessions are not signed by a trusted certificate authority; therefore they do not provide authentication. If you intend to use encrypted remote connections externally, you should consider purchasing a certificate from a trusted certificate authority.

With SSL enabled, the console and management interface perform exactly as they do when SSL is disabled.

When SSL is enabled for the VMware Virtual Machine Console, a lock icon appears in the lower right corner of the console window. Any consoles that are already open at the time SSL is enabled do not become encrypted, and the lock icon does not appear in these console windows. You must close these consoles and start new console sessions to ensure encryption.

When SSL is enabled for the VMware Management Interface, the URL to connect to the management interface is `https://<hostname>:8333`. The management interface automatically redirects users to this URL if they use the insecure URL (`http://<hostname>:8222`) to connect. A lock icon appears in the status bar of the browser window.

If you disable SSL, users are automatically redirected to `http://<hostname>:8222` if they use `https://<hostname>:8333` to connect to the management interface.

Note: If SSL is disabled then enabled again, any new management interface connections to the non-secure port (8222) are not redirected.

Using Your Own Security Certificates

If you prefer, you can use your own security certificate when you enable SSL.

On a Windows host, run the Microsoft Management Console (`mmc.exe`) and select your certificate. When you upgrade the VMware Management Interface on a GSX Server for Windows host, you need to reassign your certificate to the management interface.

On a Linux host, the VMware Management Interface certificate must be placed in `/etc/vmware-mui/ssl`. The management interface certificate consists of two files: the certificate itself (`mui.crt`) and the private key file (`mui.key`). The private key file should be readable only by the root user.

When you upgrade the VMware Management Interface on a Linux host, the certificate remains in place and, in case you removed the management interface, the directory is not removed from your host.

Enabling and Disabling SSL for Remote Sessions

You enable and disable SSL for VMware Virtual Machine Console connections in the console or the management interface. You enable SSL for VMware Management Interface connections in the management interface. By default, SSL is enabled for all remote connections.

Remember that the certificates used in these secure sessions are not signed by a trusted certificate authority; therefore they do not provide authentication. If you intend to use encrypted remote connections externally, you should consider purchasing a certificate from a trusted certificate authority.

To change SSL settings for console and management interface connections from the VMware Management Interface, see [Securing Remote Connections with SSL on page 144](#).

To change the SSL setting for console connections from the VMware Virtual Machine Console, see [Enabling SSL for VMware Virtual Machine Console Connections on page 157](#).

Identifying a Virtual Machine by Its UUID

Each virtual machine is automatically assigned a universally unique identifier (UUID), which is stored in the SMBIOS system information descriptor. It can be accessed by standard SMBIOS scanning software — for example SiSoftware Sandra or the IBM utility `smbios2` — and used for system management in the same way you use the UUID of a physical computer.

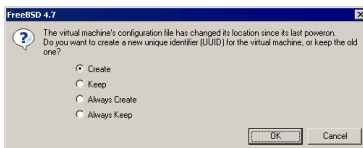
The UUID is a 128-bit integer. The 16 bytes of this value are separated by spaces, except for a dash between the eighth and ninth hexadecimal pairs. So a sample UUID looks like this:

```
00 11 22 33 44 55 66 77-88 99 aa bb cc dd ee ff
```

The UUID is based on the physical computer's identifier and the path to the virtual machine's configuration file. This UUID is generated when you power on or reset the virtual machine. As long as you do not move or copy the virtual machine to another location, the UUID remains constant.

If you move or copy the virtual machine, you have the choice of creating a new UUID the first time you power on the virtual machine. This new UUID is based on the physical computer's identifier and path to the virtual machine's configuration file in its new location.

When you power on a virtual machine that was moved or copied to a new location, a message appears.



If you moved this virtual machine, you can choose to keep the UUID. Select **Keep**, then click **OK** to continue powering on the virtual machine.

If you copied this virtual machine to a new location, you should create a new UUID, since the copy of the virtual machine is using the same UUID as the original virtual machine. Select **Create**, then click **OK** to continue powering on the virtual machine.

If the original virtual machine is being used as a template for more virtual machines, you can choose to create a new UUID the first time you power on each copy. After you configure the virtual machine and are ready to make it a template, move it to a new location and power it on. When the message appears after you power on, select **Always Create**, then click **OK** to continue powering on the virtual machine. The virtual

machine is set up to create a new UUID every time it is moved. Power off the virtual machine and begin using it as a template by copying the virtual machine files to other locations.

If you intend to move the virtual machine numerous times, and want to keep the same UUID each time the virtual machine moves, then select **Always Keep** and click **OK** to continue powering on the virtual machine.

Note: If you want to change the Always Keep or Always Create setting, power off the virtual machine and edit its configuration file (.vmx). Delete the line that contains

```
uuid.action = "create"
```

or

```
uuid.action = "keep"
```

Suspending and resuming a virtual machine does not trigger the process that generates a UUID. Thus, the UUID in use at the time the virtual machine was suspended remains in use when the virtual machine is resumed, even if it has been copied or moved. However, the next time the virtual machine is rebooted, the message appears, so you can choose to create a new UUID or keep the existing one.

Specifying a UUID for a Virtual Machine

In some circumstances you may want to assign a specific UUID to the virtual machine. To do this, you need to override the automatically generated UUID value. Power off the virtual machine and edit its configuration file (.vmx) to set the value of the UUID parameter. Use a text editor to edit the configuration file. The format for the line is:

```
uuid.bios = <uuidvalue>
```

The UUID value must be surrounded by quotation marks. A sample configuration line looks like:

```
uuid.bios = "00 11 22 33 44 55 66 77-88 99 aa bb cc dd ee ff"
```

After adding this line to the configuration file, power on the virtual machine. The new UUID is used when the virtual machine boots.

Logging GSX Server Events on Windows

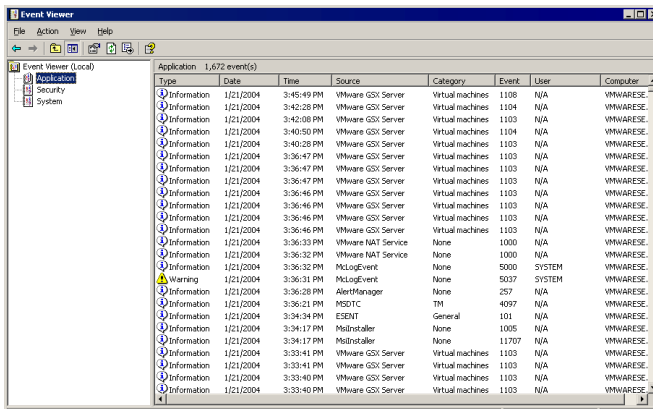
GSX Server sends information about events that occur in the application to the Event Viewer on Windows hosts. Each event has a unique identifier to assist you in tracking various events with automation tools.

The types of events that are sent to the Event Viewer include:

- Any changes to a virtual machine's power state. When a virtual machine is powered on or off, suspended or resumed, an entry is logged in the Event Viewer.
- The addition or removal of virtual machines from the inventory.
- The deletion of a virtual machine from the GSX Server system.
- Any messages and warnings generated by GSX Server and the responses to these messages and warnings. Whenever GSX Server generates a message or a warning prompt to which the user must respond, the message or warning and the user's response are logged in the Event Viewer. A message or a warning is any dialog box that GSX Server generates in the application that is not a hint.

To access the Event Viewer, choose **Start > Administrative Tools > Event Viewer**.

Select the **Application** log to view GSX Server events.



You can modify the information that gets logged for a particular machine or for all virtual machines. The two options you can modify include:

- `eventlog.win.message=FALSE` — this setting prevents the logging of all dialog box and message events that appear in GSX Server.

- `eventlog.win.register=FALSE` — this setting prevents the logging of power state change events and logging of when a virtual machine is added to or removed from the inventory.

To modify what gets logged for a virtual machine, add either or both of the options to the virtual machine's configuration (`.vmx`) file.

To modify what gets logged for all virtual machines on a host, add either or both of the options to the `GSX Server config.ini` file, located by default in `C:\Documents and Settings\All Users\Application Data\VMware\VMware GSX Server`.

Backing Up Virtual Machines

This section discusses methods for backing up your virtual machines and the GSX Server host.

Using a Backup Agent in the Virtual Machine

The best way to back up virtual machines that require constant uptime (24 hours a day, seven days a week) is to load a backup agent in each virtual machine. This agent should connect directly through your network to your backup servers. This method allows you to completely back up individual files on your virtual machines and recover files individually.

Supported Backup Configurations

VMware has tested the following backup software in virtual machines using the Dell PowerVault 120T tape drive/changer:

- BrightStor ARCserve Backup version 9.0 (build 1868)
- Veritas Backup Exec 9, Service Pack 1

The tape drive must be configured as a generic SCSI device. To add the drive to a virtual machine, see [Adding a Generic SCSI Device to a Virtual Machine](#) in the *VMware GSX Server Virtual Machine Guide*.

Note: If the virtual machine has a Windows guest operating system installed and is configured to use the BusLogic SCSI adapter, then you must use the VMware BusLogic driver, available from the VMware Web site at www.vmware.com/download.

Using a Backup Agent Running on the Host Operating System

Another backup method uses a backup agent running on the GSX Server host. You back up a virtual machine by suspending and resuming it with batch files containing `vmware-cmd` commands. Suspending a virtual machine puts it in a state in which the host backup software can gain exclusive access to the virtual machine files to complete its task.

Your suspend batch file should contain the following line:

```
vmware-cmd <path_to_config>\<config>.vmx suspend
```

Once the virtual machine is suspended, you can safely back up this virtual machine's directory using the backup agent installed on the GSX Server host.

After the backup job completes, you would run a resume batch job to restart the virtual machine. The batch file should contain the following line:

```
vmware-cmd <path_to_config>\<config>.vmx start
```

This command resumes the virtual machine into an active, running state.

If you want to restore a virtual machine to a server other than the GSX Server host where it was originally located, shut down the virtual machine. Instead of using the suspend batch file, use one that powers off the virtual machine.

```
vmware-cmd <path_to_config>\<config>.vmx stop
```

The suspend, stop and resume commands can be used in pre- and post-job scripts that are normally available via the backup software being used. Backup software such as Veritas Backup Exec has the capability to run pre- and post-batch jobs with scheduled backups.

Backing Up the GSX Server Host

To completely back up your entire GSX Server environment for a given point in time, back up your entire GSX Server host. Shut down all virtual machines on the host, then back up the host and all virtual machine directories. However, restoring a virtual machine directory from such a backup returns you to that point in time; you cannot restore individual files in the virtual machine.

Considerations for Backing Up Virtual Machines

A virtual machine directory should not be backed up on the GSX Server host if the virtual machine is powered on. You should either suspend or shut down the virtual machine before backing up its directory.

If the virtual machine is running when you try to back it up, the virtual machine can hang and be unreachable.

Open file agents loaded on the GSX Server host do not always work reliably when you back up open virtual disks that are gigabytes in size.

Before implementing a backup method, test and document the method in advance to ensure a successful backup.

For more information on scripting and using the `vmware-cmd` file, read Appendix A of the *VMware Scripting API User's Manual*, available on the VMware Web site at www.vmware.com/pdf/Scripting_API_21.pdf.

Using the VMware Management Interface

GSX Server provides the VMware Management Interface, a Web-based management tool that allows you to

- Monitor the state of virtual machines and the GSX Server host on which they are running.
- Control (power on, suspend, resume, reset and power off) the virtual machines on that host.
- Connect the VMware Virtual Machine Console to a given virtual machine, for hands-on management.
- View details about each virtual machine, including system summary, hardware information, any connected users and a log of recent events.
- Modify virtual machine configurations.
- Create and delete virtual machines.
- Secure console and management interface sessions with SSL (administrator and root users only).
- Answer questions and acknowledge messages posed by the virtual machine.

In order for a user to manage a virtual machine from the VMware Management Interface, that user must have at least read permission for that virtual machine's configuration file. For more information about permissions and GSX Server, see [Understanding Permissions and Virtual Machines on page 106](#).

To properly view the VMware Management Interface, you should ensure that style sheets are enabled in your browser, regardless of which browser and version you are using.

Note: If you intend to run the VMware Management Interface in Internet Explorer 6.0 on a Windows Server 2003 system, whether the GSX Server host is installed on Windows Server 2003 or a Windows Server 2003 client machine that connects to a GSX Server host, you need to follow some special configuration steps in order to use the management interface. For more information, see [Configuring Web Browsers for Use with GSX Server on page 61](#).

The VMware Management Interface starts with a Login page, where you enter your user name and password to log in. The Login page contains links for downloading the

VMware Virtual Machine Console for Windows and Linux hosts. For more information, see [Downloading the VMware Virtual Machine Console on page 104](#).

Once your user name and password are authorized by the management interface, the Status Monitor page appears. The Status Monitor page contains high level details about all the virtual machines on the host server to which you are connected. The Status Monitor page links to a detailed set of pages specific to each virtual machine, where you find information about virtual devices, configuration options and a summary of recent events. In addition, you can create and delete virtual machines from your browser.

These pages refresh or reload automatically every 90 seconds. You may want to refresh or reload these pages manually before you perform an operation like suspending, resuming, or powering on or off a virtual machine from the management interface — or after you perform a power operation in a console — in case another user has performed the same or a conflicting operation right before you. To refresh the page, click Refresh at the top of a page.

Setting the Session Length for the VMware Management Interface

Your management interface sessions times out after 60 minutes of idle time.

On a Windows host, this setting is specified by the variable

`vmware_SESSION_LENGTH`, stored in `C:\Program`

`Files\VMware\VMware Management Interface\htdocs\init.pl`.

You can change this setting to any number of minutes, or you can block access to the management interface for all users by setting `vmware_SESSION_LENGTH` to 0 minutes. You can have persistent sessions that never time out by setting `vmware_SESSION_LENGTH` to -1.

On a Linux host, you can change this setting by running the management interface configuration program `vmware-config-mui.pl`. You can block access to the management interface for all users by setting the timeout length to 0 minutes. You can have persistent sessions that never time out by setting the timeout length to -1.

Logging In to the VMware Management Interface

To use the VMware Management Interface, you should be running a supported browser (Internet Explorer 5.5 or 6.0 — VMware highly recommends using 6.0, Netscape Navigator 7.0 or Mozilla 1.x). You need to know the host name or IP address of the server you want to manage. You must have a valid user name and password on that server.

You can connect to the server with up to eight management interface sessions at a time.

The URL to connect to the server is `https://<hostname>:8333`.

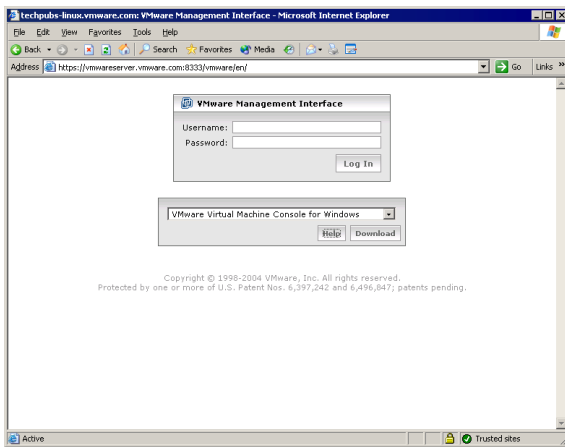
Note: If you are connecting to the management interface from a browser on the host machine, you can use `localhost` as the `<hostname>`.

Note: If you disabled SSL for your management interface sessions, the URL to connect to the server is `http://<hostname>:8222`. For more information, see [Securing Your Remote Sessions on page 112](#).

Note: If you disabled SSL, users are automatically redirected to `http://<hostname>:8222` if they use `https://<hostname>:8333` to connect to the management interface.

Note: If you are using Netscape Navigator or Mozilla, check the advanced preferences (**Edit > Preferences > Advanced**) to be sure JavaScript and style sheets are both enabled.

Enter the URL. The Login page appears.



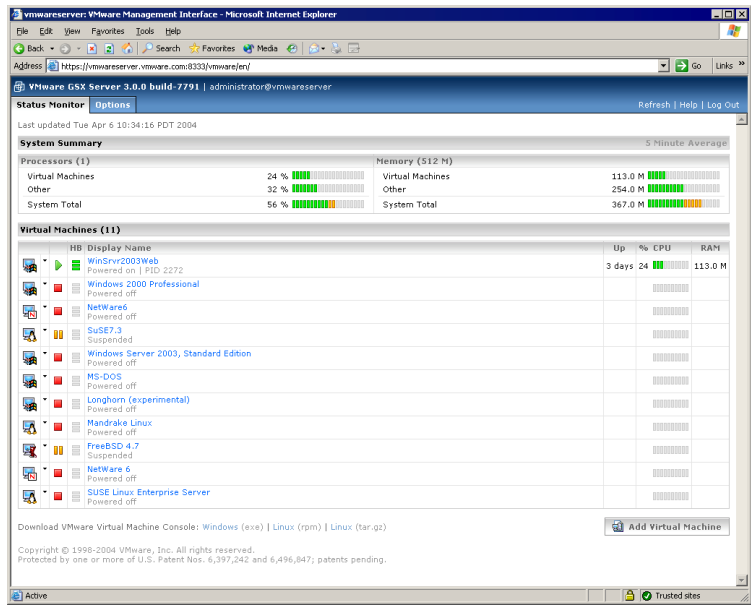
The Login page contains fields for your user name and password.

It also contains a menu so you can download installation packages for the VMware Virtual Machine Console. To download a package, see [Downloading the VMware Virtual Machine Console on page 104](#).

On the Login page, enter your user name and password for the host machine, then click **Log In**. The Status Monitor page appears.

Using the Status Monitor

The Status Monitor page contains a high-level view of the GSX Server host including a host system summary and list of all virtual machines known to the host that you have sufficient permissions to see.



Viewing Summary Information about the GSX Server Host System

Under **System Summary**, you can view:

- The number of processors on the GSX Server host, including the average percentage of CPU usage used by virtual machines, other processes on the host and the total being used by the whole system for the previous minute.
- The amount of memory on the GSX Server host, including the average amount of memory used by virtual machines, other processes on the host and the total being used by the whole system for the previous minute.

Viewing Summary Information about Virtual Machines on the Host

Under **Virtual Machines**, you can view a list of all virtual machines known to the host that you have sufficient permissions to see. When a virtual machine is running, the Status Monitor page displays its ID number after the power status of the virtual machine.

Activities you can perform include:

- [Connecting to a Virtual Machine with the VMware Virtual Machine Console on page 125](#)
- [Using the Virtual Machine Menu on page 126](#)
- [Changing the Power State of a Virtual Machine on page 127](#)
- [Monitoring the Virtual Machine's Heartbeat on page 128](#)
- [Viewing Information about a Virtual Machine on page 129](#)
- [Downloading the VMware Virtual Machine Console on page 104](#) (Login and Status Monitor pages)
- [Creating a New Virtual Machine from the VMware Management Interface](#) in the *VMware GSX Server Virtual Machine Guide* (Status Monitor page only)
- [Deleting a Virtual Machine Using the VMware Management Interface on page 142](#)
- [Configuring the GSX Server Host on page 143](#) (Options page only)
- [Using Common Controls on page 129](#)

Connecting to a Virtual Machine with the VMware Virtual Machine Console

If you need to view a particular virtual machine's desktop, you can attach the VMware Virtual Machine Console and connect to the virtual machine. Click the terminal icon () to launch the console. For more information on connecting the console, see [Connecting to a Virtual Machine on a Windows Host](#) and [Connecting to a Virtual Machine on a Linux Host](#) in the *VMware GSX Server Virtual Machine Guide*.

Note: If you are connecting an older version of a console to the server, you need to select the virtual machine after you connect to the server host. VMware recommends you update the console on this client. Download the appropriate installer on the Login or Status Monitor page. See [Downloading the VMware Virtual Machine Console on page 104](#).

Netscape and Mozilla users must define a MIME type for the console first; Internet Explorer is automatically configured when the console is installed. For more information, see [Setting a MIME Type to Launch the VMware Virtual Machine Console on page 157](#).

The terminal icon appears slightly different, depending upon the guest operating system selected for the virtual machine when it was created. This visual cue helps to identify the virtual machine (for example, the display name may not indicate the guest operating system). The variations in the terminal icon are shown here.

-  — indicates a Windows guest operating system.
-  — indicates a Linux guest operating system.
-  — indicates a FreeBSD guest operating system.
-  — indicates a NetWare guest operating system.
-  — indicates another guest operating system, such as MS-DOS.

Using the Virtual Machine Menu

Click the arrow to the right of the terminal icon () to display a menu of options for that virtual machine. The menu includes the following commands, most of which can be performed using the buttons and other visual elements of the management interface.

Depending on your permissions and the state of the virtual machine, some options may not be available.

- **Attach Console** — launches the VMware Virtual Machine Console, which connects to this virtual machine. Selecting this option is the same as clicking . You need to log in to the host. For more information, see [Connecting to a Virtual Machine on a Windows Host](#) and [Connecting to a Virtual Machine on a Linux Host](#) in the *VMware GSX Server Virtual Machine Guide*.

Note: Netscape and Mozilla users must define a MIME type for the console first; Internet Explorer is automatically configured when the console is installed. For information, see [Setting a MIME Type to Launch the VMware Virtual Machine Console on page 157](#).

- **Properties** — opens the Virtual Machine Overview page for this virtual machine in a new browser window. Selecting this option is the same as clicking the virtual machine name link in the **Display Name** column.
- **Configure Hardware** — opens the Hardware page, where you can edit a virtual machine's hardware configuration. You can edit most configuration options only when the virtual machine is powered off. When the virtual machine is powered on, you can edit removable devices and the virtual network adapter.

For more information, see [Configuring a Virtual Machine's Hardware on page 132](#).

- **Configure Options** — opens the Options page, where you can edit a virtual machine's configuration, such as the guest operating system type, display name, the location of the suspended state file and the startup and shutdown options.

With the exception of the display name, you can edit these options only when the virtual machine is powered off.

For more information, see [Setting Standard Virtual Machine Configuration Options on page 134](#).

- **Shut Down Guest** — runs the script associated with this power state change, then shuts down the guest operating system and powers off the virtual machine. Selecting this option is the same as clicking  in the power state popup.
- **Suspend after Running Script** — runs the associated script then suspends a running virtual machine. Selecting this option is the same as clicking  in the power state popup.
- **Power On/Resume and Run Script** — powers on a stopped virtual machine or resumes a suspended virtual machine, then runs the script associated with this power state change. Selecting this option is the same as clicking  in the power state popup.
- **Restart Guest** — gracefully restarts the guest operating system and the virtual machine. Selecting this option is the same as clicking  in the power state popup.
- **Power Off** — powers off the virtual machine immediately without running a script or shutting down the guest operating system. Selecting this option is the same as turning off the power to a physical computer.
- **Suspend** — suspends a powered on virtual machine without running a script.
- **Power On/Resume** — powers on a stopped virtual machine or resumes a suspended virtual machine without running a script.
- **Reset** — resets the virtual machine immediately without running a script or stopping the guest operating system. Selecting this option is the same as pressing the reset button on a physical computer.
- **Delete Virtual Machine** — lets you delete a virtual machine and its files, provided the virtual machine is powered off. See [Deleting a Virtual Machine Using the VMware Management Interface on page 142](#).

Changing the Power State of a Virtual Machine

Depending upon your permissions, you can change the power state of the virtual machine in the management interface. Your permissions are listed in the **Users and Events** tab for the virtual machine. For more information, see [Viewing a List of Connected Users on page 139](#).

To change the virtual machine’s power state, click the button that indicates the virtual machine’s current power state. A popup menu appears, displaying the following buttons:

Button	Description
	Shuts down the guest operating system and powers off the virtual machine. Any open applications close, the guest operating system shuts down, then GSX Server powers off the virtual machine. VMware Tools executes any script associated with this power state change. When this icon is red, the virtual machine is powered off.
	Suspends a running virtual machine. VMware Tools executes any script associated with this power state change. When this icon is amber, the virtual machine is suspended.
	Powers on a stopped virtual machine or resumes a suspended virtual machine. VMware Tools executes any script associated with this power state change. When this icon is green, the virtual machine is running.
	Restarts a guest operating system. Any open applications close, the guest operating system shuts down, then GSX Server restarts the guest. VMware Tools executes any script associated with this power state change.

Changing the power state executes any script associated with the power state change. For more information about running scripts, see [Executing Scripts When the Virtual Machine’s Power State Changes](#) in the VMware *VMware GSX Server Virtual Machine Guide*.

Monitoring the Virtual Machine’s Heartbeat

Under **HB** is a bar graph that represents the average percentage of heartbeats received by a virtual machine during the previous minute. The heartbeat represents the overall health of the guest operating system, based on whether applications running in the guest are consuming resources from other applications in the guest.

The heartbeats are sent by the VMware guest operating system service to the virtual machine from its guest operating system; the percentage is relative to the number of heartbeats the virtual machine expects to receive for the minute before the page was last updated. Heavily loaded guest operating systems may not send 100% of the expected heartbeats, even though the system is otherwise operating normally; in general, only when the heartbeat percentage drops to zero should the virtual machine or guest operating system be considered abnormal.

Note: If VMware Tools is not installed or is not running, the guest operating system does not send any heartbeats to its virtual machine and this meter is disabled.

Viewing Information about a Virtual Machine

Important virtual machine information is readily available on the Status Monitor page.

- The link in the **Display Name** column indicates the display name for the virtual machine; if one is not specified, then the path to the configuration file for the virtual machine appears here instead. This column also contains the virtual machine's power state, its process ID and its virtual machine ID (if it is running); it also notes if VMware Tools is not installed.

If the virtual machine is waiting for a response to a system message, a **Waiting for input link** appears here. Click the link to view the message and respond to it.

Click the virtual machine link for more details about the virtual machine. The Virtual Machine Overview page appears in a new browser window. For more information, see [Configuring a Virtual Machine on page 130](#).

- The value in the **Up** column indicates the length of time the virtual machine has been running.
- The value in the **% CPU** column indicates the average percentage of host operating system processor capacity the virtual machine used during the final minute before the page was last updated. More detailed processor information is available on the Virtual Machine Overview page.
- The value in the **RAM** column indicates the average amount of memory the virtual machine used during the final minute before the page was last updated. More memory information is available on the Virtual Machine Overview page.

Using Common Controls

The following links appear on most or all of the pages in the management interface.

Refresh — This link refreshes or reloads the current page. To avoid conflicts with other users, click this button before you perform an operation in the management interface like shutting down, suspending, resuming or powering on a virtual machine — or **after** you perform such an operation in a console.

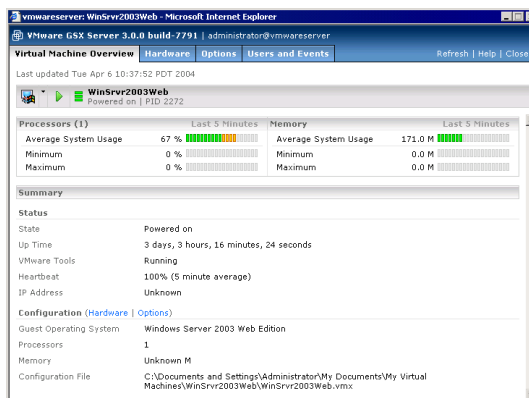
Help — This link connects you to the online documentation for the current page in the management interface.

Logout — This link logs you out of the management interface. You can log out from the Status Monitor and Options pages only. Click **Logout** to return to the Login page. See [Logging Out of the VMware Management Interface on page 141](#).

Close — This link closes the current management interface window.

Configuring a Virtual Machine

To see more information about a particular virtual machine and to modify its configuration, click the link to that virtual machine in the **Display Name** column on the Status Monitor page. The Virtual Machine Overview page appears in a new browser window.



The Virtual Machine Overview page contains the following information:

- The current power state of the virtual machine — whether it is powered on, powered off or suspended.
- The process ID of the virtual machine.
- The VMID of the virtual machine, which is the GSX Server version of the PID for a running virtual machine.
- The minimum, maximum and average percentage of GSX Server host processor capacity that the virtual machine used in the previous minute.
- The minimum, maximum and average amount of GSX Server host memory that the virtual machine used in the previous minute.
- How long the virtual machine has been running.
- The status of VMware Tools — whether VMware Tools is installed and running.
- The average percentage of heartbeats received by a virtual machine during the previous minute. See [Monitoring the Virtual Machine's Heartbeat on page 128](#).
- The IP address of the virtual machine.
- Links to edit the virtual machine's hardware and standard configuration options. Click **Hardware** to edit the virtual machine's hardware. The Hardware page

appears. Click **Options** to edit the virtual machine's standard configuration options. The Options page appears. You can make changes to the virtual machine's configuration in these places. To change most options, you must power off the virtual machine.

- The guest operating system installed in the virtual machine.
- The number of virtual processors in the virtual machine.
- The amount of memory allocated to the virtual machine.
- The path to the virtual machine's configuration file on the GSX Server host.

Activities you can perform when viewing a virtual machine's details include:

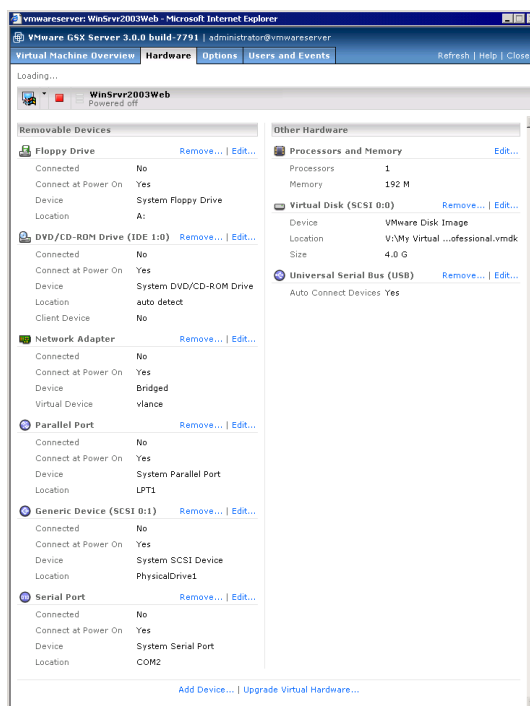
- [Connecting to a Virtual Machine with the VMware Virtual Machine Console on page 125](#)
- [Using the Virtual Machine Menu on page 126](#)
- [Changing the Power State of a Virtual Machine on page 127](#)
- [Using Common Controls on page 129](#)
- [Configuring a Virtual Machine's Hardware on page 132](#)
- [Setting Standard Virtual Machine Configuration Options on page 134](#)
- [Modifying the Configuration File Directly \(Advanced Users Only\) on page 137](#)
- [Viewing a List of Connected Users on page 139](#)
- [Viewing a Log of a Virtual Machine's Events on page 140](#)

Configuring a Virtual Machine's Hardware

To configure the virtual hardware inside a virtual machine, click the **Hardware** tab. The Hardware page appears.

The Hardware page lists the virtual hardware in the virtual machine — configured devices like the virtual disk; removable devices like floppy, CD-ROM or DVD-ROM drives; virtual network adapters and memory allocated to the virtual machine.

You can configure each virtual hardware component. Most hardware can be configured only when the virtual machine is powered off.



Activities you can perform when viewing a virtual machine's hardware include:

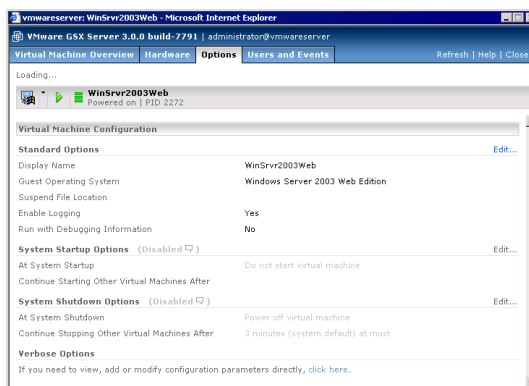
- [Configuring a Virtual Disk from the Management Interface](#) in the *VMware GSX Server Virtual Machine Guide*
- [Configuring Virtual Machine Memory from the Management Interface](#) in the *VMware GSX Server Virtual Machine Guide*
- [Configuring a Virtual Network Adapter from the Management Interface](#) in the *VMware GSX Server Virtual Machine Guide*

- [Configuring a Virtual Machine's DVD-ROM or CD-ROM Drive from the Management Interface](#) in the *VMware GSX Server Virtual Machine Guide*
- [Configuring a Virtual Machine's Floppy Drive from the Management Interface](#) in the *VMware GSX Server Virtual Machine Guide*
- [Adding a Virtual Disk from the Management Interface](#) in the *VMware GSX Server Virtual Machine Guide*
- [Adding a Virtual Network Adapter from the Management Interface](#) in the *VMware GSX Server Virtual Machine Guide*
- [Adding a DVD-ROM or CD-ROM Drive from the Management Interface](#) in the *VMware GSX Server Virtual Machine Guide*
- [Adding a Floppy Drive from the Management Interface](#) in the *VMware GSX Server Virtual Machine Guide*
- [Adding a Parallel Port from the Management Interface](#) in the *VMware GSX Server Virtual Machine Guide*
- [Adding a Serial Port from the Management Interface](#) in the *VMware GSX Server Virtual Machine Guide*
- [Connecting to an Output File from the Management Interface](#) in the *VMware GSX Server Virtual Machine Guide*
- [Connecting to an Application from the Management Interface](#) in the *VMware GSX Server Virtual Machine Guide*
- [Connecting Two Virtual Machines from the Management Interface](#) in the *VMware GSX Server Virtual Machine Guide*
- [Adding a USB Controller from the Management Interface](#) in the *VMware GSX Server Virtual Machine Guide*
- [Adding a Generic SCSI Device to a Virtual Machine from the Management Interface](#) in the *VMware GSX Server Virtual Machine Guide*
- [Removing Hardware Using the Management Interface](#) in the *VMware GSX Server Virtual Machine Guide*
- [Connecting to a Virtual Machine with the VMware Virtual Machine Console](#) on page 125
- [Using the Virtual Machine Menu](#) on page 126
- [Changing the Power State of a Virtual Machine](#) on page 127
- [Using Common Controls](#) on page 129

Click the tabs at the top of the page to view more information about the virtual machine.

Setting Standard Virtual Machine Configuration Options

To review and modify basic information about a virtual machine, or to access the configuration file directly, click the **Options** tab. The Options page appears.



The Options page displays the following virtual machine information:

- **Display Name** — identifies the virtual machine in a descriptive way.
- **Guest Operating System** — indicates the guest operating system installed on the virtual disk.
- **Suspend File Location** — specifies the location of the suspended state file; this file is created when you suspend a virtual machine. It contains information about the virtual machine's state at the time at which it was suspended. GSX Server automatically adds a `.vmss` suffix to the name of the suspended state file to ensure that one virtual machine does not overwrite the suspended state file of another.
- **Enable Logging** — indicates whether logging is enabled.
- **Run with Debugging Information** — indicates whether the virtual machine is running with debugging information. It is useful to enable this option when you are experiencing problems with this virtual machine, as you can provide this information to VMware support to help troubleshoot those problems. However, enabling this setting affects virtual machine performance.
- **At System Startup** — indicates whether or not this virtual machine should start when the server starts. By default, virtual machines do not start automatically when the system starts up.

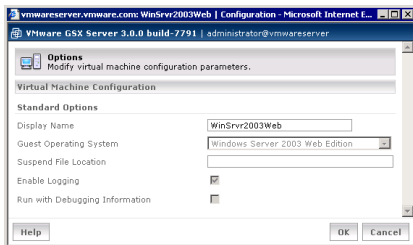
- **Continue Starting Other Virtual Machines After** — indicates the amount of time GSX Server waits after starting the virtual machine before starting another virtual machine. Settings for starting virtual machines include start when the server starts, do not wait to start, wait for a certain number of minutes to start and start when VMware Tools starts.
- **At System Shutdown, Attempt to** — sets the shutdown action for the virtual machine when the server is shut down. Settings for shutting down virtual machines include power off the virtual machine, shut down the guest operating system and suspend the virtual machine. By default, all virtual machines are powered off when the system shuts down.
- **Continue Stopping Other Virtual Machines After** — specifies the amount of time GSX Server waits after stopping the virtual machine before stopping another virtual machine. Settings for stopping virtual machines include the system default (specified in [Configuring Startup and Shutdown Options for Virtual Machines on page 145](#)), no wait or wait for a certain number of minutes.
- **Verbose Options** — allows you to enter and modify configuration file entries by hand. See [Modifying the Configuration File Directly \(Advanced Users Only\) on page 137](#).

Changing Configuration Options

To change any standard virtual machine configuration options, complete the following steps.

1. Power off the virtual machine and click **Edit**. The Options Configuration page appears.

Note: You can change the display name when the virtual machine is running.



2. To change the display name, type the new name in the **Display Name** field.
3. To change the guest operating system (for example, if you are upgrading the guest operating system installed in the virtual machine), select the new guest operating system from the **Guest Operating System** list.

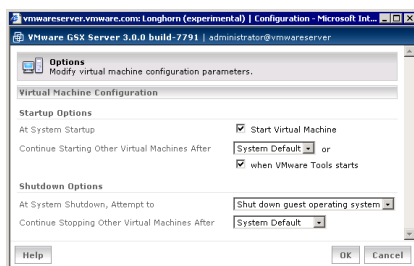
4. To change the location of the suspended state file, enter the location on the host in the **Suspend File Location** list.
5. To change whether logging is enabled for the virtual machine, check (to enable) or clear (to disable) the **Enable Logging** check box.
6. To change whether the virtual machine is running with debugging information, check (to enable) or clear (to disable) the **Run with Debugging Information** check box.
7. Click **OK** to save your changes and close the window.

Setting Virtual Machine Startup and Shutdown Options

You can configure whether a virtual machine starts when the system starts, and how it shuts down when the system shuts down. You can enable these settings as long as the startup and shutdown options are enabled for the server. See [Configuring Startup and Shutdown Options for Virtual Machines on page 145](#).

To configuring a virtual machine's startup and shutdown options, complete the following steps.

1. Power off the virtual machine and click **Edit** under **System Startup Options** or **System Shutdown Options**. The Options page appears.



2. To allow the virtual machine to start up when the system starts up, check the **Start Virtual Machine** check box.

Specify the period of time before the next virtual machine starts in the **Continue Starting Virtual Machines After** list. Choose the number of minutes or whether GSX Server should not wait before starting the next virtual machine. If you select **Other**, a prompt appears; specify in the prompt the number of minutes to wait. The **System Default** is specified in [Configuring Startup and Shutdown Options for Virtual Machines on page 145](#).

To specify that VMware Tools should start in a virtual machine before the next virtual machine starts, check the **when VMware Tools starts** check box. If

VMware Tools does not start in the virtual machine before the specified time elapses, GSX Server starts the next virtual machine.

3. Specify what happens to the virtual machine when the system shuts down. In the **At System Shutdown, Attempt to** list, select whether you want to power off the virtual machine, shut down the guest operating system or suspend the virtual machine.

Configure when GSX Server should stop the next virtual machine after this virtual machine stops in the **Continue Stopping Other Virtual Machines After** list. Choose the number of minutes, if any, that GSX Server should wait before stopping the next virtual machine. If you select **Other**, a prompt appears; specify in the prompt the number of minutes to wait. The **System Default** is specified in [Configuring Startup and Shutdown Options for Virtual Machines on page 145](#).

4. Click **OK** to save your settings.
5. Click **Close Window** to return to the virtual machine's Options page.

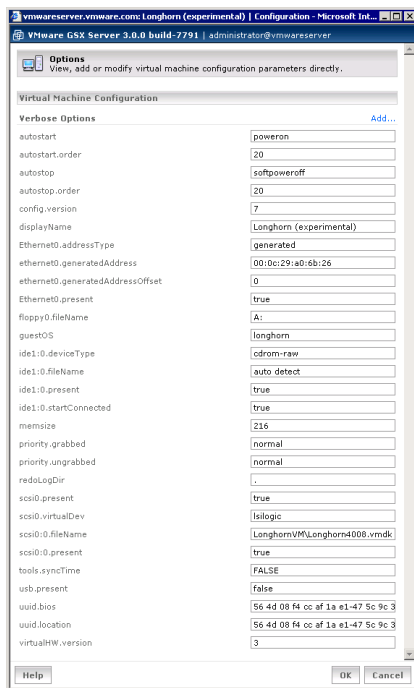
Modifying the Configuration File Directly (Advanced Users Only)

If you need to add or change a virtual machine's configuration option that cannot be accessed from elsewhere in the management interface, you can edit the virtual machine's configuration file (`.vmx`) from the **Options** tab.

Caution: You should not add or change any options in your configuration file unless you have been given specific instructions about an option in another part of the user documentation, or if you are working with VMware support to solve an issue with your virtual machine.

To add an option to the configuration file, make sure you are logged into the management interface as the virtual machine user or as a user with the proper permissions to modify this virtual machine (such as the Administrator or root user), then complete the following steps. Make sure the virtual machine is powered off.

1. Under **Verbose Options**, click the [click here](#) link. The Options page appears.



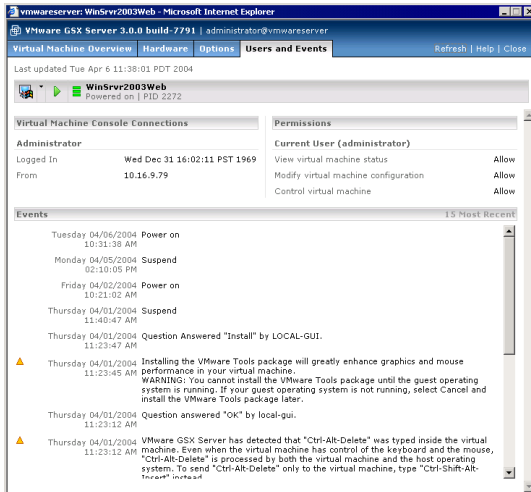
2. Click **Add**.
3. A prompt appears. Enter a name for the option, then click **OK**.
4. Another prompt appears. Enter a value for option you specified, then click **OK**.
5. Click **OK** in the Options page to save the change to the configuration file.

To change an option in the configuration file, complete the following steps.

1. Under **Verbose Options**, click the [click here](#) link. The Options page appears.
2. Locate the option you want to change, then change the value in the entry field to the right of the option.
3. Click **OK** to save your change and close the Options page.

Viewing a List of Connected Users

To see a list of users who are connected to a virtual machine with a console or VMware Scripting API, click the **Users and Events** tab.



The list under **Remote Console Connections** identifies any users connected to the virtual machine with a console or VMware Scripting API. The list includes the time and IP address from which the user connected to the virtual machine and the status of the user's activity.

The list under **Permissions** indicates what you can do with the virtual machine. You are either allowed or denied the following abilities:

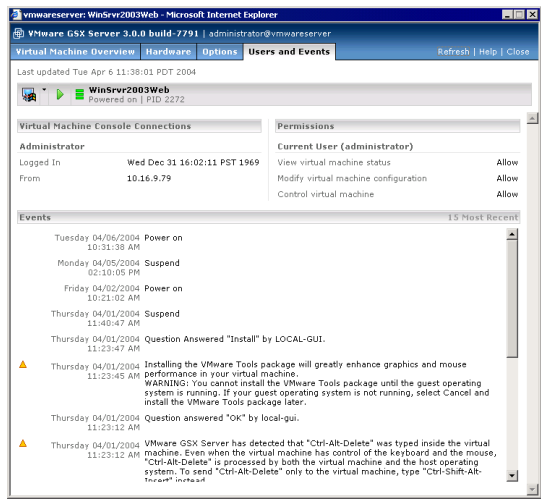
- Viewing virtual machine status.
- Modifying the virtual machine's configuration.
- Controlling the virtual machine — powering it on or off, suspending or resuming it.

Activities you can perform when viewing a virtual machine's user and event information include:

- [Connecting to a Virtual Machine with the VMware Virtual Machine Console on page 125](#)
- [Using the Virtual Machine Menu on page 126](#)
- [Changing the Power State of a Virtual Machine on page 127](#)
- [Using Common Controls on page 129](#)

Viewing a Log of a Virtual Machine’s Events

A log of the 25 most recent virtual machine events is available. Click the **Users and Events** tab. The Users and Events page appears.



The **Events** list displays a log of the most recent actions or events recorded in the virtual machine, such as the questions GSX Server asks, any errors and the powering on or off the virtual machine. Events appear in reverse chronological order; that is, the most recent events appear first in the list.

The event log draws its data from the log file for the virtual machine's configuration file. The log file is stored, by default, in the virtual machine's directory. On a Windows host, this directory is <installdrive>:\Virtual Machines\<guestOS>. On a Linux host, this directory is /var/lib/vmware/Virtual Machines/<guestOS>.

Sometimes you see a waiting for input message appears as a link in the **Display Name** column. This link appears when you perform an action in the management interface that prompts the virtual machine to generate a message; you must respond to the message before the virtual machine can proceed. When you click that link, a prompt appears, where you can enter a response. After you provide your answer, the prompt closes. Your response appears in the **Events** list.

The log shows the date and time the event occurred and an explanation of the event. Some events have a symbol associated with them that corresponds to the type of event that occurred.

▲ — This type of event indicates the virtual machine generated a question or warning.

● — This type of event indicates an error occurred in the virtual machine.

Note: On Windows hosts, the host operating system's Event Viewer tracks virtual machine power state changes, GSX Server messages and answers to prompts that appear in the virtual machine. For more information, see [Logging GSX Server Events on Windows on page 117](#).

The Apache Server and the VMware Management Interface

On GSX Server for Linux hosts, an Apache server is installed with the management interface. Listed here are the commands to start, stop and restart the Apache server.

In order to use these commands, you must first log in as root (`su -`), then open a terminal session.

To start the Apache server, type

```
/etc/init.d/httpd.vmware start
```

To stop the Apache server, type

```
/etc/init.d/httpd.vmware stop
```

To restart the Apache server, type

```
/etc/init.d/httpd.vmware restart
```

Logging Out of the VMware Management Interface

When you are ready to log out of the VMware Management Interface, click **Logout** on the Status Monitor or Options page. You are prompted to confirm that you want to log out. Logging out of the management interface does not affect the virtual machines on the host or any consoles you opened from the management interface.

VMware Management Interface sessions expire automatically after 60 minutes of inactivity or idle time. To change the session length, see [Setting the Session Length for the VMware Management Interface on page 122](#).

Deleting Virtual Machines

You can delete a virtual machine only if you are the Administrator or root user. You may want to delete a virtual machine if it is no longer needed or if you need to free up disk space on your host.

When you delete a virtual machine, the files associated with it — that is, all files located in the same directory — and the virtual machine's directory are deleted. The files include the virtual machine's configuration file (`.vmx`), log file, `nvrAm` file, suspended state file and snapshot file.

Any virtual disks that are associated with another virtual machine on the host are **not** deleted. The directory containing these files is not deleted.

You delete virtual machines from the VMware Virtual Machine Console and the VMware Management Interface.

Deleting a Virtual Machine Using the VMware Virtual Machine Console

To use the console to delete a virtual machine, make sure the virtual machine is powered off. Select its tab in the virtual machine display or select it in the inventory, then choose **VM > Delete from Disk**. You are prompted to confirm your action. Click **Yes** to delete the virtual machine.

Deleting a Virtual Machine Using the VMware Management Interface

To use the management interface to delete a virtual machine, complete the following steps.

1. In the VMware Management Interface, find the virtual machine you want to delete. If the virtual machine is powered on, power it off. If it is suspended, resume it, then power it off.
2. Access the virtual machine menu. Click the arrow to the right of the terminal icon (.
3. Choose **Delete Virtual Machine**. A message informs you that this deletes all virtual machine files. Click **OK** to allow GSX Server to delete the virtual machine and all its files.

Note: If you do not want to delete this virtual machine, click **Cancel**.

Configuring the GSX Server Host

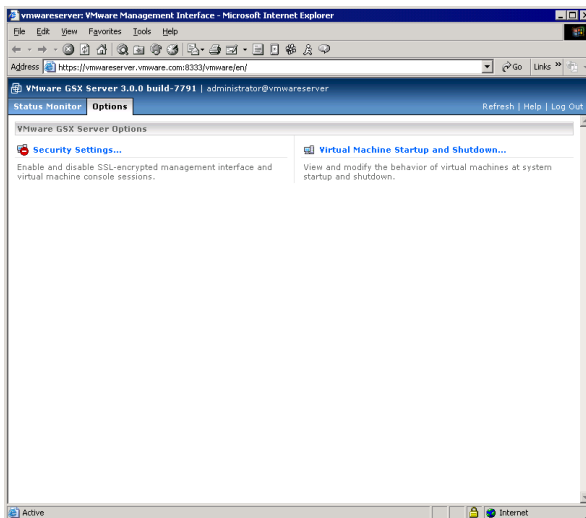
Configuring the GSX Server host involves:

- [Configuring GSX Server from the Management Interface on page 143](#)
- [Setting User Preferences for the VMware GSX Server Host on page 149](#)
- [Setting Global Preferences for VMware GSX Server on page 154](#)
- [Setting a MIME Type to Launch the VMware Virtual Machine Console on page 157](#)

Configuring GSX Server from the Management Interface

To configure the GSX Server host from the management interface, on the Status Monitor page, click the **Options** tab. The Options page appears.

Note: Only a user with administrator privileges (Windows hosts) or the root user (Linux hosts) can access this tab.



Configuring the host from the management interface involves:

- [Securing Remote Connections with SSL on page 144](#)
- [Configuring Startup and Shutdown Options for Virtual Machines on page 145](#)

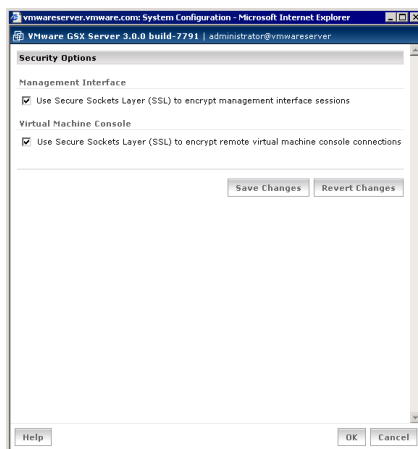
Securing Remote Connections with SSL

VMware Management Interface sessions and VMware Virtual Machine Console connections are secured with SSL. For more information about SSL, see [Securing Your Remote Sessions on page 112](#).

You can enable SSL for console connections from the console itself. For details, see [Enabling SSL for VMware Virtual Machine Console Connections on page 157](#).

To configure SSL from the management interface, complete the following steps.

1. Log in to the VMware Management Interface as the Administrator (GSX Server for Windows hosts) or root user (GSX Server for Linux hosts).
2. On the Status Monitor page, click the **Options** tab. The Options page appears.
3. Click **Security Settings**. The Security Settings page appears.



4. To secure your management interface sessions, check the **Use Secure Sockets Layer (SSL) to encrypt management interface sessions** check box.
5. To secure your console connections, check the **Use Secure Sockets Layer (SSL) to encrypt remote console connections** check box.

Note: If you change the SSL setting for the management interface, the system automatically logs you out and must log in again.

6. To save your settings, click **OK**.

When SSL is enabled, a lock icon appears in the status bar of the browser running the VMware Management Interface, and in the status bar of the VMware

Virtual Machine Console window, unless the console is connected to a virtual machine on the local host.

After you change your SSL setting for the management interface, you are prompted to accept the security certificate in your browser the next time you log in to the management interface.

Configuring Startup and Shutdown Options for Virtual Machines

You can configure your host to determine if virtual machines start up or shut down when the host operating system starts or shuts down.

You can set a delay from the time one virtual machine starts or stops until the next one starts or stops. This delay helps to prevent overburdening the host, since significant processor and memory are capacities required to simultaneously start or stop multiple guest operating systems.

You can determine the global order in which virtual machines start and stop.

The host is configured to start and stop virtual machines automatically by default. You can customize the global settings and virtual machine-specific settings. To customize these settings for a virtual machine, see [Setting Virtual Machine Startup and Shutdown Options on page 136](#).

The system-wide virtual machine startup and shutdown options include:

- **Start Up and Shut Down Virtual Machines** — determines whether or not virtual machines are started and stopped with the system. If enabled, default startup and shutdown policies are applied to all virtual machines on your system (where no virtual machines are powered on when the host starts and all virtual machines are shut down when the host shuts down); you can customize each virtual machine's startup and shutdown policies.

If this option is disabled, you cannot set startup and shutdown policies for any virtual machines on your system.

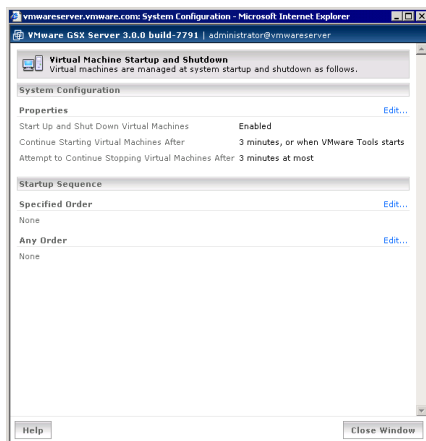
- **Continue Starting Virtual Machines After** — sets the amount of time GSX Server waits after starting one virtual machine before starting another virtual machine. You can set this so that GSX Server does not wait before starting the next virtual machine, waits a certain number of minutes before starting or starts when VMware Tools starts in the current virtual machine.
- **Attempt to Continue Stopping Virtual Machines After** — sets the amount of time GSX Server waits after stopping one virtual machine before stopping another virtual machine. You can set this so that GSX Server does not wait before

stopping each virtual machine or waits a certain number of minutes before stopping each virtual machine.

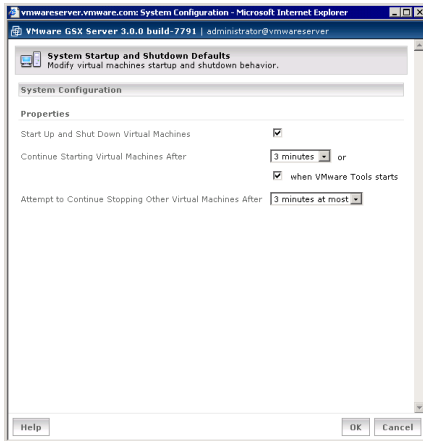
Enabling the System's Configuration Settings

To enable the system-wide configuration settings for virtual machines, complete the following steps.

1. On the Options page of the management interface, click **Virtual Machine Startup and Shutdown**. The Virtual Machine Startup and Shutdown page appears.



2. Under **System Configuration**, click **Edit**. The System Startup and Shutdown Defaults page appears.



3. To enable system-wide startup and shutdown policies, check the **Start Up and Shut Down Virtual Machines** check box.
4. To configure when GSX Server should start the next virtual machine after a virtual machine starts, do one or both of the following:
 - To specify a period of time before the next virtual machine starts, in the **Continue Starting Virtual Machines After** list, either choose the number of minutes to wait or indicate that GSX Server should not wait before starting the next virtual machine. If you select **Other**, specify the number of minutes to wait in the prompt that appears. It is a good idea to set a delay between starting virtual machines, as a delay avoids placing an undue burden on the host processors and memory.
 - To specify that VMware Tools should start in a virtual machine before the next virtual machine starts, check **when VMware Tools starts**. If VMware Tools does not start in the virtual machine before the time specified in the **Continue Starting Virtual Machines After** list elapses, GSX Server starts the next virtual machine.
5. To configure when GSX Server should stop the next virtual machine after a virtual machine stops, in the **Attempt to Continue Stopping Other Virtual Machines After** list, either choose the number of minutes to wait or indicate that GSX Server should not wait before starting the next virtual machine. If you select **Other**, specify the number of minutes to wait in the prompt that appears. It is a

good idea to set a delay between stopping virtual machines, as a delay avoids placing an undue burden on the host processors and memory.

6. Click **OK** to save your settings.
7. Click **Close Window** to return to the management interface's Options page.

Specifying the Order in Which Virtual Machines Start

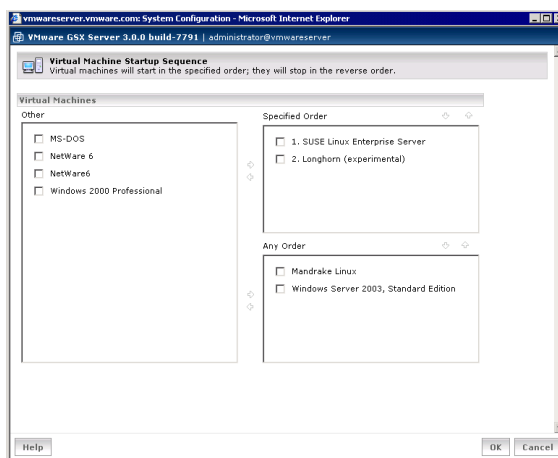
Once you set whether or not virtual machines should start and stop with the system, you can set the order in which the virtual machines start and stop. Setting the sequence allows you to specify the position of a given virtual machine in the system-wide startup and shutdown sequence. If a sequence is set for a virtual machine, the virtual machine starts and stops in of the following orders:

- **Specified Order** — lists the virtual machines in the order in which they are configured to start and stop.
- **Any Order** — lists the virtual machines specified to start and stop in any order.

You cannot specify the startup order for a virtual machine if it is configured to run as the user who powers it on. The virtual machine must be configured to run as the local system account or as a specific user.

Editing the Startup Sequence for Virtual Machines

To edit the startup sequence for virtual machines, click **Edit** under Startup Sequence. The Virtual Machine Startup Sequence configuration page appears and displays the virtual machines on your system.



To specify the startup order for the virtual machines on the host, select the check box next to one or more machines. Once you select a virtual machine, navigation arrows highlight, allowing you to move machines between the three lists. Virtual machines can be set to one of the following options:

- **Other** — lists the virtual machines that are configured to use the default start and stop policies when the system starts up and shuts down.
- **Specified Order** — lists the virtual machines in the order in which they are configured to start. The order in which the virtual machines stop is the reverse of the order in which they start, so the last virtual machine to start when the system starts up is the first to stop when the system shuts down. To specify the startup order, select machines and use the arrows to move them up or down within the list.
- **Any Order** — lists the virtual machines that are configured to start and stop in any order. Move virtual machines to this category if you want them to start and stop with the system, but you do not want to set the order for them. The virtual machines in this category do not start or stop until all the virtual machines listed in the **Specified Order** list have started or stopped.

Disabling the System's Configuration Settings

To disable the system-wide configuration settings, complete the following steps.

1. On the Virtual Machine Startup and Shutdown page, under **System Configuration**, click **Edit**. The System Startup and Shutdown Defaults page appears.
2. Clear the **Start Up and Shut Down Virtual Machines** check box, then click **OK**.
3. Click **Close Window** to return to the management interface's Options page.

Setting User Preferences for the VMware GSX Server Host

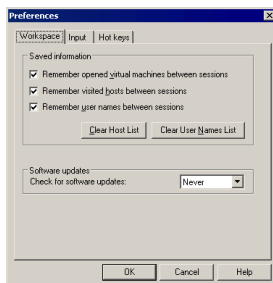
The Preferences dialog box allows you to change a number of settings that apply to all virtual machines running in a console. These settings apply to the user currently logged on to the host computer. The settings do not affect settings made by any other user when that user is logged in to the host. These settings can be changed by regular users, as well as root and Administrator users.

To change these settings, choose **Edit > Preferences**. The Preferences dialog box appears.

Setting Workspace Preferences

The **Workspace** tab lets you determine whether any virtual machines appear in the virtual machine display each time you open a console. On a Windows host, you can

specify whether any host and user names appear in the console Login dialog box when you connect. You can specify how often GSX Server should check for software updates.



If you select the **Remember opened virtual machines between sessions** check box, you see a tab for each opened virtual machine in the virtual machine display the next time you open a console. A virtual machine is considered opened if both of the following conditions are true:

- The virtual machine was left open.
- The virtual machine was powered on and off, or powered on and suspended.

If you select the **Remember visited hosts between sessions** check box, the name of any GSX Server host to which you connected in a previous console session appears in the console's Login dialog box. To clear the list of remembered hosts, click **Clear Host List**.

If you select the **Remember user names between sessions** check box, any user names you used when you connected during previous console sessions appear in the console's Login dialog box. To clear the list of remembered user names, click **Clear User Names List**.

Updating GSX Server Software Automatically

GSX Server checks automatically to see if updates for the product are available. By default, it checks once a week, and if an update is available, displays a message when you launch a console. You can check manually at any time by choosing **Help > Check for Updates on the Web**. You can change the interval for the automatic check, or switch to manual checks only.

Choose **Edit > Preferences > Workspace**. Select the interval in the **Check for software updates** drop-down list.

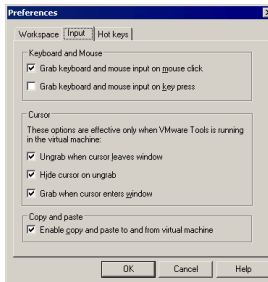
You can set the interval to never, manual (you check for updates manually), daily, weekly or monthly.

If you are running GSX Server on a Windows host behind a proxy server, make sure your browser is configured to connect to the Internet through your proxy server.

If you are running GSX Server on a Linux host behind a proxy server, make sure you configure `http_proxy` with the name of the proxy server and the port number the proxy server uses.

Changing Your Input Settings

The **Input** tab lets you adjust the way that the virtual machine captures control of the keyboard and mouse.



Note: The **Grab when cursor enters window** option allows you to move the mouse pointer back into the virtual machine window easily if you have been working in the virtual machine and temporarily moved the mouse pointer outside the virtual machine window. The mouse pointer is grabbed only when GSX Server has focus (is the active application). If you release the mouse pointer by pressing a hot-key combination — the default is Ctrl-Alt — you must click inside the virtual machine window to make GSX Server grab the mouse pointer again.

The input settings you can specify include:

- **Grab keyboard and mouse input on mouse click** — GSX Server takes control of the keyboard and the mouse after the first primary mouse button click in the virtual machine console window.
- **Grab keyboard and mouse input on key press** — GSX Server takes control of the keyboard and the mouse after the first keystroke. The first keystroke is sent to the virtual machine. When the virtual machine console window is active and this option is selected, you cannot use the normal application and system accelerator key sequences.
- **Ungrab when cursor leaves window** — the mouse pointer becomes the mouse pointer of your host operating system when the mouse pointer exits the virtual machine console window. This option does not apply when the virtual

machine is in full screen mode. Use this option to transition seamlessly between the virtual machine and your host operating system.

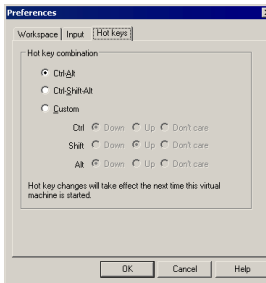
- **Hide cursor on ungrab** — the mouse pointer of the guest operating system is hidden when your mouse is controlling the pointer of the host operating system. This option is particularly useful when your guest operating system and your host operating system are identical: it eliminates the confusion of having to think about which of the two identical pointers moves when you move your mouse.
- **Grab when cursor enters window** — the mouse pointer becomes the mouse pointer of your guest operating system when the mouse pointer enters the virtual machine console window. This option does not apply when the virtual machine is in full screen mode.
- **Enable copy and paste to and from virtual machine** — use this option for copying and pasting text between the host and the virtual machine and among virtual machines. The clipboards of the two operating systems communicate with each other. When the mouse pointer of your guest operating system exits the console window, the contents of the guest operating system clipboard are copied into the host operating system clipboard. Similarly, each time the mouse pointer of your host operating system is grabbed by the console window, the contents of the host operating system clipboard are copied into the guest operating system clipboard.

Note: At this time, you cannot copy and paste between Red Hat Linux 7.0 through 7.3 and Windows 2000. It does not matter which operating system is the guest and which is the host.

Note: The best way to understand the cursor options is to play with them for a while. They describe how the mouse pointer should behave when you are in windowed mode; that is, the virtual machine is in a console window, not in full screen mode, and you can see your host operating system's desktop.

Setting Hot Key Preferences

Use the **Hot Key** tab to change which combination of keys (the Ctrl, Alt and Shift keys in combination with other keys) are passed to the guest operating system or are intercepted by GSX Server.



You can construct your own custom hot-key combination if, for example, the default Ctrl+Alt combination conflicts with another application on the host that processes the same hot-key combination.

For example, you may want to change hot key combinations from Ctrl-Alt-<key> to Ctrl-Shift-Alt-<key> to prevent GSX Server from intercepting Ctrl-Alt-Delete instead of letting the key combination be sent to the guest operating system.

Or, you may be using PC Anywhere to connect to a machine running a console. The the console is connected to a virtual machine running in full screen mode, and you want to run a different application. Normally, to return to window mode, you press Ctrl-Alt, but PC Anywhere processes Ctrl-Alt key combinations, so GSX Server cannot receive the key combination. Thus, you need to use an alternate hot-key combination to get out of full screen mode.

Note: Because Ctrl-Alt is the key combination that tells GSX Server to release (ungrab) mouse and keyboard input, combinations that include Ctrl-Alt are not passed to the guest operating system. If you need to use such a combination — for example, Ctrl-Alt-<Fkey> to switch between Linux workspaces in a virtual machine — press Ctrl-Alt-Space, release Space without releasing Ctrl and Alt, then press the third key of the key combination you want to send to the guest.

You can also construct your own custom hot-key combination. Select **Custom**, then select the combination of Ctrl, Alt and Shift keys. You specify whether each key is:

- **Down** — where you must press the key down as part of the key combination.
- **Up** — where you must leave the key unpressed as part of the key combination.
- **Don't care** — where it does not matter if you press the key.

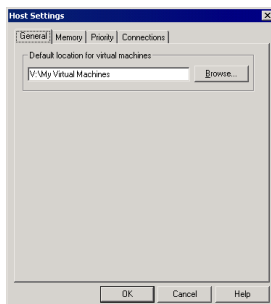
Setting Global Preferences for VMware GSX Server

The Host Settings dialog box allows you to change a number of settings that apply to VMware GSX Server itself.

To change these settings, choose **Host > Settings**. You must be either the root or Administrator user to change these settings.

Specifying Where Virtual Machines Are Created

Use the **General** tab to specify the default location where all virtual machines on this host are created.



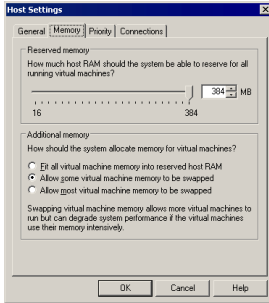
The directory GSX Server uses by default is displayed under **Default location for virtual machines**. To set a different directory, type in the path or click **Browse** to navigate to the directory you want to use. GSX Server creates a directory for each new virtual machine under the directory you specify here.

On a Windows host, the default folder where new virtual machines are stored is `<installdrive>:\Virtual Machines`.

On a Linux host, the default location where new virtual machines are stored is `/var/lib/vmware/Virtual Machines`.

Reserving Host Memory for Virtual Machines

Select the **Memory** tab to adjust the amount of memory reserved for all running virtual machines.



The settings on the Memory tab applies no matter what virtual machine is running or who is logged on to the host computer.

For more information about memory and virtual machines, see [Understanding Memory Usage on page 185](#) and [Allocating Memory to a Virtual Machine](#) in the *VMware GSX Server Virtual Machine Guide*.

Adjusting Priorities for Virtual Machine Processes (Windows Hosts Only)

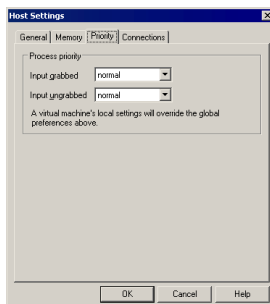
GSX Server for Windows gives you the option to set the priority that the Windows process scheduler gives to your virtual machines when mouse and keyboard input are going to a particular virtual machine and when input is not going to that virtual machine.

You can adjust these settings to improve overall system performance based on the relative priority of work you are doing in various virtual machines and on the host computer.

The settings on the Priority tab apply to all virtual machines for the user currently logged on to the host computer. The priority settings do not affect priority settings made by any other user on the computer.

There is no corresponding setting on a Linux host.

To set priority preferences, in the Host Settings dialog box, click the **Priority** tab.



The priority settings here are used by all virtual machines unless a virtual machine configuration overrides the global setting with a local setting. To change the local setting for a particular virtual machine, and override the global settings, open the virtual machine you want to adjust, choose **VM > Settings**, click the **Options** tab, select **Advanced**, then use the drop-down lists under **Process priorities** to make the setting you want for that virtual machine.

There are three possible process scheduling priorities: low, normal and high. The typical process on the host runs at normal priority. If you set the priority of the virtual machine to low, that virtual machine has lower priority than other processes on the host. If you set the priority of the virtual machine to normal, that virtual machine contends with all the processes on the host. If you set the virtual machine priority to high, that virtual machine gets priority over other processes on the host.

GSX Server gives you the option to automatically change the process scheduling priority that applies when the virtual machine grabs and ungrabs keyboard and mouse input. For more information on grabbing and ungrabbing input, see [Changing Your Input Settings on page 151](#).

The four possible process priorities are

- **high - normal:** When input is grabbed, GSX Server gets priority over other processes on the host. When input is not grabbed, GSX Server contends with all the processes on the host.
- **high - low:** When input is grabbed, GSX Server gets priority over other processes on the host. When input is not grabbed, GSX Server has lower priority than other processes on the host.
- **normal - normal:** When input is grabbed, GSX Server contends with all the processes on the host. When input is not grabbed, GSX Server contends with all the processes on the host.

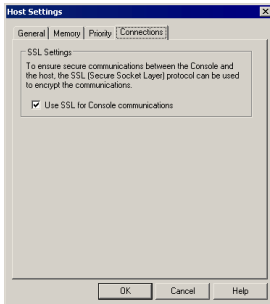
- **normal - low:** When input is grabbed, GSX Server contends with all the processes on the host. When input is not grabbed, GSX Server has lower priority than other processes on the host.

GSX Server defaults to process priority **normal - normal**.

Enabling SSL for VMware Virtual Machine Console Connections

Select the **Connections** tab to enable SSL for console connections over a network.

To enable SSL for console connections from the console, on the **Connections** tab, check the **Use SSL for Console communications** check box.



For more information about SSL, see [Securing Your Remote Sessions on page 112](#).

Setting a MIME Type to Launch the VMware Virtual Machine Console

From the VMware Management Interface, you can connect to a virtual machine from a console by clicking the terminal icon () for that virtual machine. Before doing so, Netscape and Mozilla users need to define a MIME type of `x-vmware-console` and associate it with the console program file. Internet Explorer is automatically configured when you install the console.

The procedure for setting a MIME type for the console is similar for Windows and Linux hosts. Both involve writing a short script that provides the command to launch the console.

You can choose to launch the console that was installed with GSX Server or you can launch the console that was installed from a file downloaded from the management interface.

Setting the MIME Type for the Console Installed with GSX Server

1. Open a text editor and do one of the following.
 - On a Windows host, write a short batch file called `vmwareGSX-helper.bat`. The batch file must contain the following line:
`"<path_to_vmwareGSX>" -o "%1"`
 where the default `<path_to_vmwareGSX>` is
`C:\Program Files\VMware\VMware GSX Server\vmware.exe`
 - On a Linux host, write a short shell script called `vmware-gsx-helper.sh`. The shell script must contain the following two lines:
`#!/bin/sh`
`"<path_to_vmware-gsx>" -o $1 > /dev/null 2>&1;`
 where the default `<path_to_vmware-gsx>` is
`/usr/bin/vmware.`
2. Save the file in a location of your choice.

Note: On a Linux host, change to the directory where you saved the file and give yourself permission to execute the file.

```
chmod +x vmware-gsx-helper.sh
```
3. Use the browser to connect to the server you want to manage.
4. Click the terminal icon () for the virtual machine you want to view in a console.
5. A dialog box asks what you want to do with the file. Click **Advanced**.
6. In the New Type dialog box, in the **Description of type** field, type `VMware GSX Server`.
7. In the **File extension** field, type `xvm`.
8. In the **MIME type** field, type `application/x-vmware-console`.
9. In the **Application to use** field, type the path to `vmwareGSX-helper.bat` or `vmware-gsx-helper.sh`.
10. Click **OK** twice. Your browser is now set to launch the console when you click the terminal icon in the future.

Setting the MIME Type for the Console Installed from the Management Interface Download

1. Open a text editor and do one of the following.

- On a Windows host, write a short batch file called `vmwareConsole-helper.bat`. The batch file must contain the following line:

```
"<path_to_vmwareConsole>" -o "%1"
```

where the default `<path_to_vmwareConsole>` is

```
C:\Program Files\VMware\VMware Virtual Machine  
Console\vmware.exe
```

- On a Linux host, write a short shell script called `vmware-console-helper.sh`. The shell script must contain the following two lines:

```
#!/bin/sh
```

```
"<path_to_vmware-console>" -o $1 > /dev/null 2>&1;
```

where the default `<path_to_vmware-console>` is
`/usr/bin/vmware-console`.

2. Save the file in a location of your choice.

Note: On a Linux host, change to the directory where you saved the file and give yourself permission to execute the file.

```
chmod +x vmware-console-helper.sh
```

3. Use the browser to connect to the server you want to manage.
4. Click the terminal icon () for the virtual machine you want to view in a console.
5. A dialog box asks what you want to do with the file. Click **Advanced**.
6. In the New Type dialog box, in the **Description of type** field, type `VMware Virtual Machine Console`.
7. In the **File extension** field, type `xvm`.
8. In the **MIME type** field, type `application/x-vmware-console`.
9. In the **Application to use** field, type the path to `vmwareConsole-helper.bat` or `vmware-console-helper.sh`.
10. Click **OK** twice. Your browser is now set to launch the console when you click the terminal icon in the future.

Moving and Sharing Virtual Machines

The following sections provide information on how to move your virtual machines from one host to another, or elsewhere on the same host, plus recommendations on how to share virtual machines with other users:

- [Moving a VMware GSX Server 3 Virtual Machine on page 163](#)
 - [Virtual Machines Use Relative Paths on page 163](#)
 - [Preparing Your Virtual Machine for the Move on page 163](#)
 - [Moving a Virtual Machine to a New Host on page 164](#)
- [Moving a GSX Server 2 Virtual Machine on page 166](#)
 - [Virtual Machines Use Relative Paths on page 166](#)
 - [Preparing Your Virtual Machine for the Move on page 166](#)
 - [Moving a Virtual Machine to a New Host on page 167](#)
- [Moving Older Virtual Machines on page 169](#)
 - [Preparing Your Virtual Machine for the Move on page 169](#)
 - [Preparing the New Host Machine on page 170](#)

- [Considerations for Moving Disks in Undoable Mode on page 171](#)
- [Sharing Virtual Machines with Other Users on page 173](#)

Note: When you move a virtual machine to a new host computer or to a different directory on the same host computer — or when you rename a directory in the path to the virtual machine's configuration file — VMware GSX Server generates a different MAC address for each virtual Ethernet adapter (unless you specified the MAC address manually). For additional information, see [Maintaining and Changing the MAC Address of a Virtual Machine](#) in the *VMware GSX Server Virtual Machine Guide*.

Moving a VMware GSX Server 3 Virtual Machine

What do you do if you have created a virtual machine using GSX Server 3 and you want to move it to a different computer? Or even somewhere else on the same computer? The process is not difficult, and in most cases you can even move your virtual machine from a Windows host to a Linux host — or vice versa. If the virtual machine was created under GSX Server 3, follow the directions in this section.

Note: These instructions assume that you are using a virtual disk — stored in one or more `.vmdk` files on your host computer.

It's always safest to make backup copies of all the files in your virtual machine's directory before you start a process like this.

Caution: VMware recommends you do not migrate a Red Hat Linux 7.3 or 7.2 virtual machine between hosts when one host is running on an AMD processor and the other is running on an Intel processor. For more information, read the Known Issues sections for these guest operating systems in the *VMware Guest Operating System Installation Guide*, available on the console Help menu.

Virtual Machines Use Relative Paths

The path names for all files associated with a GSX Server 3 virtual machine are relative, meaning the path to each file is relative to the currently active directory. For example, if you are in the virtual machine's directory, the relative path to the virtual disk file is `<machine name>.vmdk`.

Preparing Your Virtual Machine for the Move

1. Shut down the guest operating system and power off the virtual machine. If the virtual machine is suspended, resume it, then shut down the guest.
2. Do one of the following:
 - If you are moving the virtual machine to a new host and have a network connection between the original host machine and the new host, you are finished with the preparations on the original host. If you do not have a network connection, you need to have a way of moving the virtual disk (`.vmdk`) files from the virtual machine's directory to the new host. You could move them to a shared network directory, for example, or burn them to CD-ROMs or DVD-ROMs.

Once you know how you are going to move the virtual machine, go to [Moving a Virtual Machine to a New Host on page 164](#).

- If you are moving this virtual machine to another directory on this host, then you are ready to make the move. Copy all the files in the virtual machine's original directory to the new location. If you stored any files in directories other than the virtual machine directory, be sure to move them into a directory of the same name and same position relative to the location of the virtual machine.

Start the VMware Virtual Machine Console and open the new virtual machine you just moved. Choose **File > Open Virtual Machine**, then browse to the virtual machine's configuration (`.vmtx`) file.

Moving a Virtual Machine to a New Host

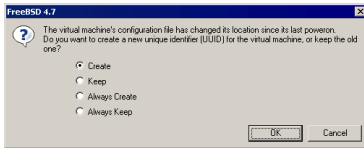
1. Make sure GSX Server is installed and working correctly on the new host.
2. Create a directory on the new host for the virtual machine you are moving. Locate the virtual disk files you are moving and copy them into the new directory. Be sure to copy all the files in the virtual machine's original directory. If you stored any files in directories other than the virtual machine directory, be sure to move them into a directory of the same name and same position relative to the location of the virtual machine. Set permissions on the directory so that it is accessible to all users of the virtual machine.

If, for some reason, you are **not** moving a file, make sure you do not have any paths pointing to that file. Use the virtual machine settings editor and check to see if your virtual machine is pointing to the correct location for files (choose **VM > Settings**) you do not move. In the virtual machine settings editor, select each device and be sure that any devices with associated files are pointed to the correct files. Also, check the Options tab to be sure the location for the redo-log file is correct.

Note: If you have taken a snapshot of the virtual machine, you can simplify the move by removing the snapshot — or reverting to the snapshot, then removing it. If you want to keep the snapshot, be sure to move the redo-log (`.REDO`) files along with all the other files in the virtual machine's directory.

3. Launch the VMware Virtual Machine Console and open the virtual machine you just moved. Choose **File > Open Virtual Machine**, then browse to the virtual machine's configuration (`.vmtx`) file.

4. The first time you power on the virtual machine, you are asked to keep the existing UUID or create a new one.



If you are using the UUID for management purposes, you should select **Keep**, then click **OK** to continue powering on the virtual machine. For more information about the UUID, see [Identifying a Virtual Machine by Its UUID on page 115](#).

Moving a GSX Server 2 Virtual Machine

If you want to move a virtual machine created with GSX Server 2, you may prefer to upgrade it for full compatibility with GSX Server 3 before moving it. To do so, run the virtual machine under GSX Server 3 and use **VM > Upgrade Virtual Hardware**. If you upgrade the virtual hardware, you can then follow the instructions in [Moving a VMware GSX Server 3 Virtual Machine on page 163](#).

If you upgrade the virtual machine, you can no longer run it under GSX Server 2. If you need to run the virtual machine under both GSX Server 2 and GSX Server 3, do not upgrade the virtual hardware. Follow the instructions in this section.

Note: These instructions assume that you are using a virtual disk — stored in one or more `.vmdk` files on your host computer.

It's always safest to make backup copies of all the files in your virtual machine's directory before you start a process like this.

Virtual Machines Use Relative Paths

The path names for all files associated with a virtual machine created under GSX Server 2 are relative, meaning the path to the each file is relative to the currently active directory. For example, if you are in the virtual machine's directory, the relative path to the virtual disk file is

```
<machine name>.vmdk.
```

If you intend to move virtual machines created in a VMware product other than GSX Server 2 or higher, or Workstation 3.1 or higher, see [Moving Older Virtual Machines on page 169](#).

Preparing Your Virtual Machine for the Move

1. Use GSX Server 2 to connect to the virtual machine. If the virtual machine has more than one virtual disk and if the virtual disks use different disk modes, you must use the Configuration Editor (choose **Settings > Configuration Editor**) to change one or more of the virtual disks so they all use the same mode.
2. Be sure the guest operating system is completely shut down. If the virtual machine is suspended and its virtual disks are in persistent or nonpersistent mode, resume it, then shut down the guest operating system.
3. If your virtual machine is using disks in undoable mode, it is best to commit or discard the changes when the guest operating system shuts down. If you cannot commit or discard the changes to your disk, read [Considerations for Moving Disks in Undoable Mode on page 171](#).

4. Do one of the following:

- If you are moving the virtual machine to a new host and have a network connection between the original host machine and the new host, you are finished with the preparations on the original host. If you do not have a network connection, you need to have a way of moving the virtual disk (`.vmdk`) files from the virtual machine's directory to the new host. You could move them to a shared network directory, for example, or burn them to CD-ROMs or DVD-ROMs.

Once you know how you are going to move the virtual machine, go to [Moving a Virtual Machine to a New Host](#) below.

- If you are moving this virtual machine to another directory on the same host, you are ready to make the move. Copy all the files in the virtual machine's original directory to the new location. If you stored any files in directories other than the virtual machine directory, be sure to move them into a directory of the same name and same position relative to the location of the virtual machine.

Launch the console and open the virtual machine you just moved. Choose **File > Open**, then browse to the virtual machine's configuration (`.vmx`) file.

Moving a Virtual Machine to a New Host

1. Make sure GSX Server is installed and working correctly on the new host.
2. Locate the virtual disk files you are moving and copy them into the new virtual machine directory. Be sure to copy all the files in the virtual machine's original directory. If you stored any files in directories other than the virtual machine directory, be sure to move them into a directory of the same name and same position relative to the location of the virtual machine. Set permissions on the directory so that it is accessible to all users of the virtual machine.

If, for some reason, you are **not** moving a file, make sure you do not have any relative or absolute paths pointing to that file. Use the virtual machine settings editor and check to see if your virtual machine is pointing to the correct location for files you do not move. In the virtual machine settings editor, select each device and be sure that any devices with associated files are pointed to the correct files. Also, check the Options tab to be sure the location for the redo-log file is correct.

In addition, check to see you do not have any absolute paths pointing to any files you **are** moving.

Note: If your virtual machine is using disks in undoable mode, it is best to commit or discard the changes when you shut down the guest operating system under GSX Server 2. If you cannot commit or discard the changes to your disk, read [Considerations for Moving Disks in Undoable Mode on page 171](#).

3. Launch the VMware Virtual Machine Console and open the virtual machine you just moved. Choose **File > Open Virtual Machine**, then browse to the virtual machine's configuration (.vmx) file.

Moving Older Virtual Machines

If you have created a virtual machine using GSX Server 1 or another VMware product (not including VMware Workstation 3.1 and later), you must upgrade the virtual hardware the first time you run it under GSX Server 3. Once you have done this, you can follow the instructions in [Moving a VMware GSX Server 3 Virtual Machine on page 163](#).

If you have created a virtual machine using GSX Server 1 or another VMware product (not including VMware Workstation 3.1 and later), and you want to move it to a different computer or to another directory on your host, you need to perform the following tasks.

Note: These instructions assume that you are using a virtual disk — stored in a set of `.vmdk` or `.disk` files on your host computer.

It is always safest to make backup copies of all the files in your virtual machine's directory before you start a process like this.

Virtual Machines May Use Relative or Absolute Paths

In GSX Server 1, the path names for all files associated with a virtual machine were absolute, or fully qualified, meaning the complete route to the files on the host was stored. For example, the absolute path to a virtual disk file might be `C:\Documents and Settings\<user name>\My Documents\My Virtual Machines\<machine name>\<machine name>.vmdk`.

With GSX Server 2 and higher, path names to files are relative, meaning the path to the each file is relative to the currently active directory. For example, if you are in the virtual machine's directory, the relative path to the virtual disk file is `<machine name>.vmdk`.

Preparing Your Virtual Machine for the Move

1. Use GSX Server 1 to open the virtual machine. If the virtual machine has more than one virtual disk and if the virtual disks use different disk modes, you must use the Configuration Editor (choose **Settings > Configuration Editor**) to change one or more of the virtual disks so they all use the same mode.
2. Be sure you know whether the virtual disk is set up as an IDE disk or a SCSI disk. You can check this in the virtual machine settings editor.

Also, note the size of the virtual disk you are moving. You need this information when you prepare the new host machine, as described in the next section.

3. Be sure the guest operating system is completely shut down. If the virtual machine is suspended, resume it using the VMware product with which you created the virtual machine, then shut down the guest operating system.

Note: Do not move a suspended virtual machine from one host to another.

4. If your virtual machine is using disks in undoable mode, it is best to commit or discard the changes when the guest operating system shuts down. If you cannot commit or discard the changes to your disk, read [Considerations for Moving Disks in Undoable Mode on page 171](#).
5. If you have a network connection between the original host machine and the new host, you are finished with the preparations on the original host. If you do not have a network connection, you need to have a way of moving the virtual disk (.vmdk) files from the virtual machine's directory to the new host. You could move them to a shared network directory, for example, or burn them to CD-ROMs or DVD-ROMs.

Note: If your disks are using undoable mode and you have not committed or discarded your changes, you must also move the redo-log (.REDO) file to the new host computer.

Preparing the New Host Machine

1. Make sure GSX Server 3 is installed and working correctly on the new host.
2. Start the VMware Virtual Machine Console and run the New Virtual Machine Wizard. Select the appropriate guest operating system for the virtual machine you are moving.

Choose a virtual disk for your hard drive and use a drive type (IDE or SCSI) that matches the type of the virtual disk you plan to move.

Select all appropriate network, floppy and CD-ROM settings. Do not make any changes with the virtual machine settings editor at this point.

Save your settings and close the virtual machine settings editor.

3. In the directory just created for the new virtual machine, delete the brand new .vmdk files that were just created.
4. Locate the virtual disk files you are moving and copy them into the new virtual machine directory. Set permissions on the directory so that it is accessible to all users of the virtual machine.

Note: If your virtual machine is using disks in undoable mode and you did not commit or discard your changes before the move, you must also move the redo-log (.REDO) file to the new host computer.

5. In the console's Inventory, select the virtual machine you just created, then choose **VM > Settings**.
6. Be sure the virtual machine is configured to use the virtual disk files you moved from the original host. You need to confirm that the new disk's settings — IDE or SCSI and the file name for the first `.vmdk` file — match those that were used on the original host machine.

The device listing for the hard drive shows whether it is SCSI or IDE. If that setting does not match the virtual disk you are moving, select the hard disk and click **Remove**. Then click **Add** and use the Add Hardware Wizard to add an IDE or SCSI disk as appropriate. Be sure to specify IDE or SCSI when you reach the Select a Disk Type screen in the wizard.

Be sure the filename and path for the virtual disk match the actual filename and location for the first `.vmdk` file used by the virtual machine you are moving.

Considerations for Moving Disks in Undoable Mode

Once you commit or discard changes made to a disk in undoable mode, you can move your disk between Linux and Windows host operating systems. You can also move your disk to different locations on your computer and to other computers with the same host operating system.

However, if you cannot or do not want to commit or discard the changes made to your undoable disk, note the following:

- You can always move a disk in undoable mode between host operating systems of the same general type (for example, between two Microsoft Windows systems, or between two Linux systems). Depending upon how the disk was first set up, you may have to place the disk and its redo log in a directory that has a path name identical to that of the current directory.
- You may be able to move the disk in undoable mode between Windows and Linux host systems, or move the disk to a different directory on your current system, if there is no path name information in the virtual machine's configuration file. This is true for virtual machines created under GSX Server 2 or higher; however, virtual machines created with older versions of GSX Server, with versions of Workstation older than 3.1 or with any other VMware product contain full path names.

Follow these steps to check the configuration and see whether or not you can move your undoable disk without committing or discarding changes:

1. Launch a GSX Server 2 console.

If you are moving a disk in undoable mode from one computer to another computer, launch a GSX Server 2 console on the computer that currently has your disk.

2. Open the configuration file for the virtual machine that uses the undoable mode disk you wish to move.

In the console window, select **File > Open** and choose the configuration file of the virtual machine with the disk you want to move.

3. Open the Configuration Editor. Choose **Settings > Configuration Editor**.
4. Examine the entry for your virtual disk to see whether it includes a full path to the first virtual disk file. For example, on a Windows host, you might see a disk file listing like this:

```
My Documents\My Virtual Machines\Windows 2000\Windows 2000.vmdk
Entries for SCSI disks are similar.
```

If your disk file information resembles the example above (with a full path to the first disk file) and you have not committed or discarded changes to the undoable disk, the following rules apply:

- You can move the disk to another computer of the same type only (Windows to Windows or Linux to Linux). You cannot move the disk to a computer of a different type (Windows to Linux or vice versa).
- You must place the virtual machine's other files (including `.vmx` and `.REDO` on Windows, and `.vmx` or `.cfg` and `.REDO` on Linux) in the same relative location on the new computer. In other words, if the virtual machine's files reside in `My Documents\My Virtual Machines\Windows 2000\` on the original host computer, you must place them in that same location on the new host computer.
- You cannot move the disk to another directory on the current system.

If your disk file information does not contain a path, it looks like this:

```
Windows 2000.vmdk
```

If your disk entry resembles the one above (just a filename with a `.vmdk` extension), you can move the disk and redo log anywhere you wish.

Sharing Virtual Machines with Other Users

If you intend to have other users access your virtual machines, you should consider the following points:

- On Windows hosts, the virtual machine files should be in a location on a system that is accessible to those users. When you configure the virtual machine in the New Virtual Machine Wizard, you can specify a location for the virtual machine elsewhere on your system or on the network.
- On Linux hosts, permissions for the virtual machine files — especially the configuration file (`.vmx`) and virtual disks (`.vmdk`) — should be set for other users according to how you want them to use the virtual machine. For instance, if you want users to run a virtual machine but not be able to modify its configuration, do not make the configuration file writable.
- If your virtual machine was created under GSX Server 3 or another VMware product (such as Workstation 4 or later) and uses independent disks in nonpersistent mode, consider changing the location of the redo-log file, since by default it is placed in your TEMP directory, to which other users may not have access. To change the location of the redo-log file, take the following steps.
 - a. With the virtual machine powered off, open the virtual machine settings editor. Choose **VM > Settings**.
 - b. Click the **Options** tab.
 - c. Click **Browse** and select a directory that is shared with other users.
 - d. Click **OK** to save the change and close the virtual machine settings editor.

Note: GSX Server 2 virtual machines with disks in nonpersistent mode perform better when the redo-log files for those disks are located in the system's TEMP directory.

- The virtual machine must be located in a directory with permissions set so that it is accessible to all users of the virtual machine.
- The virtual machine must not be private. For more information, see [Only You Can See a Virtual Machines You Create on page 107](#).

6

CHAPTER

Performance Tuning and the VMware GSX Server Host

The following sections offer suggestions for getting the best performance from VMware GSX Server and your virtual machines:

- [Configuring and Maintaining the Host Computer on page 176](#)
- [Configuring GSX Server on page 177](#)
 - [General GSX Server Options on page 177](#)
 - [GSX Server on a Windows Host on page 181](#)
 - [GSX Server on a Linux Host on page 184](#)
- [Understanding Memory Usage on page 185](#)
 - [Memory Use on the Host on page 185](#)
 - [Specifying How Much RAM is Used by All Running Virtual Machines on page 185](#)
 - [Memory Usage on Older Linux Hosts on page 188](#)

Configuring and Maintaining the Host Computer

You may see slower virtual machine performance if the physical disk that holds the virtual machine's working directory or the physical disk that holds the virtual disk files is badly fragmented. By default, the working directory holds the virtual disk files and is on the host computer. If you have customized the virtual machine configuration, you may have placed the working directory or the virtual disk files on a different physical computer.

Fragmentation of the host disk can affect any or all of the following:

- The files that hold a virtual disk
- The files that store newly saved data when you take a snapshot
- The files that hold information used in suspending and resuming a virtual machine

If you are experiencing slow disk performance in the virtual machine, or if you want to improve the speed of suspend and resume operations, check to be sure the host disk that holds the virtual machine's working directory and virtual disk files is not badly fragmented. If it is fragmented, you can improve performance by running a defragmentation utility to reduce fragmentation on that host disk.

Configuring GSX Server

This section offers advice and information about factors that can affect the performance of GSX Server itself. This section does not address performance of the guest operating system or the host operating system.

Note: In addition to the GSX Server configuration options discussed below, you should always install VMware Tools in any guest operating system for which a VMware Tools package exists. Installing VMware Tools provides better video and mouse performance and also greatly improves the usability of the virtual machine. For details, see [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide*.

General GSX Server Options

The following sections describe ways you can improve the performance of GSX Server on both Windows and Linux hosts.

Guest Operating System Selection

Make certain you select the correct guest operating system for each of your virtual machines. To check the guest operating system setting, choose **VM > Settings > Options > General**.

GSX Server optimizes certain internal configurations on the basis of this selection. For this reason, it is important to set the guest operating system correctly. The optimizations can greatly aid the operating system they target, but they may cause significant performance degradation if there is a mismatch between the selection and the operating system actually running in the virtual machine. (Selecting the wrong guest operating system should not cause a virtual machine to run incorrectly, but it may degrade the virtual machine's performance.)

Memory Settings

Make sure to choose a reasonable amount of memory for your virtual machine. Many modern operating systems have a growing need for memory, so assigning a generous amount is beneficial for the best virtual machine performance.

The same holds true for the host operating system, especially a Windows host.

The New Virtual Machine Wizard automatically selects a reasonable starting point for the virtual machine's memory, but you may be able to improve performance by adjusting the settings in the virtual machine settings editor (choose **VM > Settings > Memory**).

If you plan to run one virtual machine at a time most of the time, a good starting point is to give the virtual machine half the memory available on the host.

Adjusting the reserved memory settings may also help. Choose **Host > Settings > Memory**.

For additional information, see [Understanding Memory Usage on page 185](#).

Debugging Mode

You can configure each virtual machine to run in one of two modes — normal mode and a mode that provides extra debugging information. The debugging mode is slower than normal mode.

For normal use, make sure the virtual machine is not running in debugging mode. Choose **VM > Settings > Options** and select **Advanced**. Under **Settings**, make sure the **Run with debugging information** check box is cleared.

CD-ROM Drive Polling

Some operating systems — including Windows NT and Windows 98 — poll the CD-ROM drive every second or so to see whether a disc is present. (Doing this allows them to run autorun programs.) This polling can cause GSX Server to connect to the host CD-ROM drive, which can make the CD-ROM drive spin up while the virtual machine appears to pause.

If you have a CD-ROM drive that takes especially long to spin up, there are two ways you can eliminate these pauses.

- You can disable the polling inside your guest operating system. The method varies by operating system. For recent Microsoft Windows operating systems, the easiest way is to use TweakUI from the PowerToys utilities.

For information on finding TweakUI and installing it in your guest operating system, go to www.microsoft.com and search for TweakUI. Specific instructions depend on your operating system.

- Another approach is to configure your virtual CD-ROM drive to be disconnected when the virtual machine starts. The drive appears in the virtual machine, but it always appears to contain no disc (and GSX Server does not connect to your host CD-ROM drive).

To make this change, go to **VM > Settings**. Select the DVD/CD-ROM item in the **Device** list. Then clear the **Connect at Power On** check box.

When you want to use a CD-ROM in the virtual machine, go to the **VM > Removable Devices** menu and connect the CD-ROM drive.

Disk Options

The various disk options (SCSI versus IDE) and types (virtual or physical) affect performance in a number of ways.

Inside a virtual machine, SCSI disks and IDE disks that use direct memory access (DMA) have approximately the same performance. However, IDE disks can be very slow in a guest operating system that either cannot use or is not set to use DMA.

The easiest way to configure a Linux guest to use DMA for IDE drive access is to install VMware Tools (**VM > Install VMware Tools**). Among other things, the installation process automatically sets IDE virtual drives to use DMA.

In Windows Server 2003, Windows XP and Windows 2000, DMA access is enabled by default. In other Windows guest operating systems, the method for changing the setting varies with the operating system. See the following technical notes in the *VMware GSX Server Virtual Machine Guide* for details.

- [Disk Performance in Windows NT Guests on Multiprocessor Hosts](#)
- [Windows 95 and Windows 98 Guest Operating System Performance Tips](#)

When a snapshot exists, virtual disks often have very good performance for random or nonsequential access. But they can potentially become so fragmented that performance is affected. In order to defragment the disk, you must first remove the snapshot (**Snapshot > Remove Snapshot**).

When no snapshot exists, physical disks and preallocated virtual disks both use flat files that mimic the sequential and random access performance of the underlying disk. When a snapshot exists and you have made changes since powering on the virtual machine, any access to those changed files performs at a level similar to the performance of a virtual disk that does not have all space allocated in advance. If you remove the snapshot, performance is again similar to that of the underlying disk.

Overall, if no snapshot exists and you are using physical disks or preallocated virtual disks, you see somewhat better performance than that provided by other configurations.

Disk writes may be slower for virtual disks that do not have all space allocated in advance. However, you can improve performance for these disks by defragmenting them from the virtual machine settings editor. Choose **VM > Settings**, select the disk you want to defragment, then click **Defragment**.

Remote Disk Access

Whenever possible, do not use disks that are on remote machines and accessed over the network unless you have a very fast network. If you must run disks remotely, choose **VM > Settings > Options**, select **General** and set the **Working directory** to a directory on your local hard disk. Then take a snapshot. After you take the snapshot, changes you make are stored locally in the working directory.

Snapshots

If you do not need to use snapshots, it is best to run your virtual machine without a snapshot. This provides best performance. To be sure a virtual machine has no snapshot, choose **Snapshot > Remove Snapshot**.

Issues Installing or Running Applications in a Guest Operating System

You may notice that whenever you try to install or start a particular program in a virtual machine, the program seems to hang, crash or complain that it is running under a debugger. VMware has seen this problem with a few programs, including the installer for the Japanese version of Trend Micro Virus Buster, the FoxPro database, the NetWare client in Windows 98, Mathcad, The Sims and Civilization III.

You can work around this problem by using a special setting called disabling acceleration. Frequently, the problem occurs only during installation or early in the program's execution; in that case you should turn acceleration back on after getting past the problem. Follow these steps:

1. Power on the virtual machine.
2. Before running or installing the program that was encountering problems, disable acceleration.

Choose **VM > Settings > Advanced** and check **Disable acceleration**.

3. Click **OK** to save the change and close the virtual machine settings editor.
4. Start the program or run the installer.
5. After you pass the point where the program was encountering problems, return to the virtual machine settings editor and remove the check beside **Disable acceleration**. You may be able to run the program with acceleration after it is started or installed.

Note: Disabling acceleration can help you get past the execution problem, but it causes the virtual machine to run slowly. If the problem occurs only at startup or during installation, you can improve performance by resuming accelerated operation after the program that was encountering problems is running or is installed.

GSX Server on a Windows Host

Note: The items in this section describe performance of GSX Server on a Windows host. For tips on configuring GSX Server on a Linux host, see [GSX Server on a Linux Host on page 184](#).

Monitoring Virtual Machine Performance

GSX Server incorporates a set of counters that work with Microsoft's Performance console to allow for the collection of performance data from running virtual machines.

Note: The Performance console is available only on Windows hosts. You cannot monitor performance for virtual machines on Linux hosts. However, you can monitor the performance of any guest operating system on the Windows host, including Linux guests.

The GSX Server performance counters can monitor the following data from a running virtual machine:

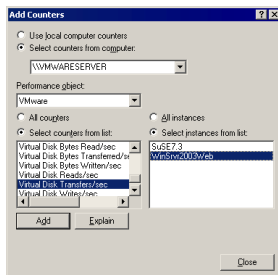
- Reading and writing to virtual disks
- Memory used by the virtual machine
- Virtual network traffic

You can track virtual machine performance only when the VMware Virtual Machine Console is open or when a virtual machine is running. The performance counters reflect the state of the virtual machine, not the guest operating system. For example, the counters can record how often the guest reads from a virtual disk, but they cannot know how many processes are running inside the guest. An explanation of each counter appears in the Performance console.

To add counters to track virtual machine performance, use the Windows Performance console. Complete the following steps.

1. Choose **Start > Programs > Administrative Tools > Performance**. The Performance console opens.

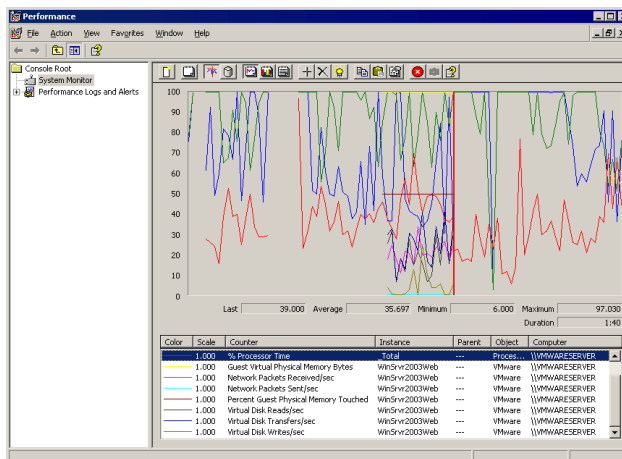
2. Select **System Monitor**, then click the plus (+) sign on the toolbar, or press **Ctrl+I**. The Add Counters dialog box appears.



3. In the **Performance object** list, select **VMware**.
4. Decide whether you want to add all counters or select one or more counters from the list.
5. To use these counters for all running virtual machines, select **All instances**. To use the counters for specific virtual machines, click **Select instances from list**, then select the virtual machines you want.

Note: For a brief description of each counter, click **Explain**. When you select a counter from the list, a description appears below the Add Counters dialog box.

6. Click **Add** to add the counters to the Performance console.



For more information about using the Performance console, use the console's in-product help or visit the Microsoft Web site.

Using Full Screen Mode

Full screen mode is faster than window mode. If you do not need to have your virtual machine and your host sharing the screen, try switching to full screen mode.

Note: You see the most noticeable improvement using full screen mode when the guest is in VGA mode. VGA mode is any mode in which the screen is in text mode (DOS, for example, or Linux virtual terminals), or 16-color 640 x 480 graphics mode (for example, the Windows 95 or Windows 98 clouds boot screen, or any guest operating system that is running without the SVGA driver provided by VMware Tools).

GSX Server on a Linux Host

Note: The items in this section describe performance of GSX Server on a Linux host. For tips on configuring GSX Server on a Windows host, see [GSX Server on a Windows Host on page 181](#).

Using Full Screen Mode

Full screen mode is faster than window mode. If you do not need to have your virtual machine and your host sharing the screen, try switching to full screen mode.

Note: You see the most noticeable improvement using full screen mode when the guest is in VGA mode. VGA mode is any mode in which the screen is in text mode (DOS, for example, or Linux virtual terminals), or 16-color 640 x 480 graphics mode (for example, the Windows 95 or Windows 98 clouds boot screen, or any guest operating system that is running without the SVGA driver provided by VMware Tools).

On a Linux host, full screen VGA mode uses the underlying video card directly, so graphics performance is quite close to that of the host. By contrast, window mode VGA requires more computer resources to emulate than window mode SVGA. As a result, if you need to run for an extended period of time in VGA mode (for example, when you are installing an operating system using a graphical installer) you should see a significant performance boost if you run in full screen mode.

Swap Space and /tmp

The amount of swap space on your host and the size of your `/tmp` directory affect performance.

For information on configuring swap space and the `/tmp` directory, read VMware Knowledge Base article 844 at www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=844.

Understanding Memory Usage

GSX Server allows you to set the memory size of each virtual machine and the amount of the host computer's memory that can be used for virtual machines. A third control governs the extent to which you want to allow the host operating system's memory manager to swap virtual machines out of physical RAM.

By adjusting these settings, you can affect both virtual machine and overall system performance.

This section describes how GSX Server uses the memory configuration parameters to manage virtual machines and system memory properly. For information on memory use for a specific virtual machine, see [Allocating Memory to a Virtual Machine](#) in the *VMware GSX Server Virtual Machine Guide*.

Memory Use on the Host

Host operating systems do not behave well when they run low on free memory for their own use. When a Windows or Linux host operating system does not have enough RAM for its own use, it thrashes — constantly swaps parts of itself between RAM and its paging file on disk. To help guard against virtual machines causing the host to thrash, GSX Server enforces a limit on the total amount of RAM that may be consumed by virtual machines.

In general, the sum of the memories of all currently running virtual machines plus overhead for the GSX Server processes cannot exceed the amount of physical memory on the host minus some memory that must be kept available for the host. For more information, see [Using Additional Memory on page 186](#).

Some memory must be kept available on the host to ensure the host is able to operate properly while virtual machines are running. The amount of memory reserved for the host depends on the host operating system and the size of the host computer's memory.

Specifying How Much RAM is Used by All Running Virtual Machines

You can set the amount of host RAM that GSX Server is allowed to reserve for all running virtual machines. To set this parameter, choose **Host > Settings > Memory**.

The reserved memory setting specifies a maximum amount of host RAM that GSX Server is allowed to use. But this memory is not allocated in advance. Even if multiple virtual machines are running at the same time, GSX Server may be using only a fraction of the RAM you specified here. Any unused RAM is available for use by other

applications. If all the RAM you specify here is in use by one or more virtual machines, the host operating system cannot use this memory itself or allow other applications to use it.

Virtual Machine Overhead

Virtual machines require relatively large amounts of memory to operate with reasonable performance. An individual virtual machine can use at most the amount of memory specified in its configuration file plus some overhead. The amount of overhead memory required depends upon the size of the guest’s virtual disks, its behavior and the amount of memory allocated to the virtual machine. Refer to the table below for the typical upper limit needed, based on the amount of memory allocated to the guest.

Amount of Memory Allocated to the Virtual Machine	Additional Amount of Overhead Needed
Up to 512MB	Up to 54MB
Up to 1000MB	Up to 62MB
Up to 2000MB	Up to 79MB
Up to 3600MB	Up to 105MB

The amount of RAM actually used for a particular virtual machine varies as a virtual machine runs. If multiple virtual machines run simultaneously, they work together to manage the memory.

The recommended amount of RAM to specify for all running virtual machines is calculated on the basis of the host computer’s physical memory and is displayed in the memory settings slider control — **Host > Settings > Memory**. If you want GSX Server to use more or less physical memory, use this slider to change the amount.

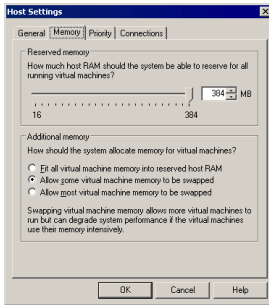
If you set this value too high, the host may thrash when other applications are run on the host. If you set this value too low, virtual machines may perform poorly and you cannot run as many virtual machines at once.

Using Additional Memory

By default, GSX Server limits the number of virtual machines that can run at once based on the amount of memory specified in the Host Settings dialog box. This limit prevents virtual machines from causing each other to perform poorly. If you try to

power on a virtual machine and there is not enough memory available, a warning appears and the virtual machine fails to power on.

To increase the number or memory size of virtual machines that can run, adjust the amount of virtual machine memory that the host operating system may swap to disk. To change this setting, choose **Host > Settings > Memory** and choose an option under **Additional memory**.



Select one of the following options:

- **Fit all virtual machine memory into reserved host RAM** — Strictly apply the reserved memory limit set in the top of the dialog box. This setting imposes the tightest restrictions on the number and memory size of virtual machines that may run at a given time. Because the virtual machines are running entirely in RAM, they have the best possible performance.
- **Allow some virtual machine memory to be swapped** — Allow the host operating system to swap a moderate amount of virtual machine memory to disk if necessary. This setting allows you to increase the number or memory size of virtual machines that can run on the host computer at a given time. It may also result in reduced performance if virtual machine memory must be shifted between RAM and disk.
- **Allow most virtual machine memory to be swapped** — Allow the host operating system to swap as much virtual machine memory to disk as it wants. This setting allows you to run even more virtual machines with even more memory than the intermediate setting does. In this case, too, performance may be lower if virtual machine memory must be shifted between RAM and disk.

If you try to power on a virtual machine and there is not enough memory available, GSX Server displays a warning message. The message shows how much memory the virtual machine is configured to use and how much memory is available. You can try

to power on the virtual machine using the available memory by clicking **OK**. If you do not want to power on the virtual machine, click **Cancel**.

Memory Usage on Older Linux Hosts

By default, Linux kernels in the 2.2.x series support 1GB of physical memory. If you want to use more memory in Linux, you can take one of several approaches.

- Upgrade to a 2.4.x series kernel that allows for more physical memory.
- Recompile your kernel as a 2GB kernel using the CONFIG_2GB option.
- Enable the CONFIG_BIGMEM option to map more physical memory. (This approach requires special steps, described in detail in the Workarounds section below, to work with VMware products.)

The CONFIG_2GB option calls for recompiling your kernel as a 2GB kernel. You do this by recompiling your kernel with CONFIG_2GB enabled. Recompiling allows Linux to support nearly 2GB of physical memory by dividing the address space into a 2GB user section and 2GB kernel section (as opposed to the normal division of 3GB for user and 1GB for kernel).

The third approach uses the CONFIG_BIGMEM option in Linux. With the CONFIG_BIGMEM option enabled, the kernel does not directly address all of physical memory and it can then map 1GB (or 2GB) of physical memory into the address space at a time. This allows the use of all of physical memory at the cost of changing the semantics the kernel uses to map virtual to physical addresses. However, VMware products expect physical memory to be mapped directly in the kernel's address space and thus do not work properly with the CONFIG_BIGMEM option enabled.

Workarounds

If you are using a 1GB kernel with CONFIG_BIGMEM enabled and have 960MB to 1983MB of memory, GSX Server does not run. To work around this issue, you can either:

- Recompile the kernel as a 2GB kernel by enabling the CONFIG_2GB option. This allows for 100 percent use of physical memory.
- Pass the boot-time switch `mem=959M` at the LILO prompt, or add it to `lilo.conf`, to disable CONFIG_BIGMEM and thus allow you to run GSX Server. To do this:

To pass the switch at the LILO prompt, type
`linux-2.2.16xxx mem=959M`

To edit `lilo.conf`, open the file in a text editor. In the `kernel` section, add this line:

```
append mem="959M"
```

If you have a 1GB kernel with `CONFIG_BIGMEM` enabled and have more than 1983MB of memory, you can do one of the following:

- Recompile the kernel as a 2GB kernel by enabling the `CONFIG_2GB` option and either pass the boot-time switch `mem=1983M` at the LILO prompt or add it to `lilo.conf`. To use the switch:

To pass the switch at the LILO prompt, type

```
linux-2.2.16xxx mem=1983M
```

To edit `lilo.conf`, open the file in a text editor. In the `kernel` section, add this line:

```
append mem="1983M"
```

- Pass the boot-time switch `mem=959M` at the LILO prompt or add it to `lilo.conf` to disable `CONFIG_BIGMEM`. To use the switch:

To pass the switch at the LILO prompt, type

```
linux-2.2.16xxx mem=959M
```

To edit `lilo.conf`, open the file in a text editor. In the `kernel` section, add this line:

```
append mem="959M"
```

If you are using a 2GB kernel with `CONFIG_BIGMEM` enabled and have 1984MB or more memory, GSX Server does not run. You can either pass the boot-time switch `mem=1983M` at the LILO prompt, or add it to `lilo.conf` to disable `CONFIG_BIGMEM` and thus allow you to run GSX Server. To use the switch:

To pass the switch at the LILO prompt, type

```
linux-2.2.16xxx mem=1983M
```

To edit `lilo.conf`, open the file in a text editor. In the `kernel` section, add this line:

```
append mem="1983M"
```


High-Availability Configurations with VMware GSX Server

The following sections describe using high-availability configurations with GSX Server:

- [Using SCSI Reservation to Share SCSI Disks with Virtual Machines on page 192](#)
- [Overview of Clustering with GSX Server on page 197](#)
 - [Applications That Can Use Clustering on page 198](#)
 - [Clustering Software in Virtual Machines on page 198](#)
- [Creating a Cluster in a Box on page 199](#)
- [Using Network Load Balancing with GSX Server on page 208](#)
- [Creating Two-Node Clusters Using Novell Clustering Services on page 213](#)

Using SCSI Reservation to Share SCSI Disks with Virtual Machines

GSX Server permits the sharing of a preallocated virtual disk with multiple virtual machines running on the same host, provided the disk in question is a SCSI disk.

When the disk is shared, all virtual machines connected to the disk use the SCSI reservation protocol to write to the disk concurrently.

Clustering software must be installed in each virtual machine that intends to share a SCSI disk. Enabling SCSI reservation in and of itself does not automatically mean that a running virtual machine is a participant in the SCSI reservation protocol.

Note: Although physical disks can be used with SCSI reservation, such use is considered experimental. Only the use of preallocated virtual disks is fully supported with SCSI reservation. When you create a new virtual machine, or add a new virtual disk to an existing virtual machine, GSX Server creates a preallocated virtual disk by default.

Note: This feature is advanced; use it only if you are familiar with SCSI in general and the SCSI reservation protocol in particular.

The following sections describe how to use SCSI reservation to share disks among multiple virtual machines.

- [SCSI Reservation Support on page 193](#)
- [Enabling SCSI Reservation on page 194](#)
- [Issues to Consider When Sharing Disks on page 196](#)

SCSI Reservation Support

SCSI reservation support is limited by the following:

- You can enable SCSI reservation for SCSI virtual and physical disks. No other type of SCSI devices can use SCSI reservation in a virtual machine. Specifically, you **cannot** enable SCSI reservation for a generic SCSI disk.

Note: VMware supports SCSI reservation when used with preallocated virtual disks. Support for SCSI reservation with physical disks is considered experimental. For high-availability configurations, use SCSI reservation with preallocated virtual disks.

- SCSI disks can be shared via SCSI reservation among virtual machines running on the same host. This means that the configuration files for the virtual machines must all be located on the same GSX Server host. However, the disk or disks the virtual machines are sharing can be located remotely on a different host.
- Even though the virtual disk is a SCSI disk, it can be located on a host running on an IDE drive. A physical disk must always be a SCSI disk.
- GSX Server virtual machines currently support only the SCSI-2 disk protocol, and not applications using SCSI-3 disk reservations. All popular clustering software (including MSCS and VCS) currently use SCSI-2 reservations.

Enabling SCSI Reservation

SCSI reservation must be enabled in a virtual machine before you can share its disks. To enable SCSI reservation, make sure the virtual machine is powered off. Open the configuration file (`.vmx`) in a text editor and add the line:

```
scsi<n>.sharedBus = "virtual"
```

anywhere in the file, where `<n>` is the SCSI bus (controller) being shared.

VMware recommends you set up the shared disks on their own SCSI bus, which is a different bus than the one the guest operating system uses. For example, if your guest operating system is on the `scsi0` bus, you should set up disks to share on the `scsi1` or `scsi2` bus.

To enable SCSI reservation for devices on the `scsi1` bus, add the following line to the virtual machine's configuration file:

```
scsi1.sharedBus = "virtual"
```

This allows the whole bus to be shared and is quicker than specifying each disk separately. However, if you do not want to share the whole bus, you can selectively enable SCSI reservation for a specific SCSI disk on the shared bus. This prevents the locking of that disk. Add the following line to the configuration file:

```
scsi1:1.shared = "true"
```

If SCSI reservation is enabled (that is, `scsi1.sharedBus` is set to `"virtual"`), then this setting is ignored.

In addition to enabling SCSI reservation on the bus, you need to allow virtual machines to access the shared disk concurrently. Add the following line to the virtual machine's configuration file:

```
disk.locking = "false"
```

This setting permits multiple virtual machines to access a disk concurrently. Be careful though: if any virtual machine not configured for SCSI reservation tries to access this disk concurrently, then the shared disk is vulnerable to corruption or data loss.

Caution: This setting applies to all SCSI devices in the virtual machine.

When SCSI reservation is enabled, the system creates a reservation lock file that contains the shared state of the reservation for the given disk. The name of this file consists of the filename of the SCSI disk appended with `.RESLCK`.

For example, if the disk `scsi1:0.filename` is defined in the configuration file as

```
scsi1:0.fileName = "<path_to_config>/vmSCSI.vmdk"
```

then the reservation lock file for this disk has the default name

```
<path_to_config>/vmSCSI.vmdk.RESLCK
```

You can provide your own lock file name. Add a definition for

`scsi1:0.reslckname` to the configuration file. For example, if you add

```
scsi1:0.reslckname = "/tmp/scsi1-0.reslock"
```

to the configuration file, this name overrides the default lock file name.

Selecting the Disk

Once SCSI reservation is enabled for a disk — that is, the `scsi[n].sharedBus = "virtual"` and `disk.locking = "false"` settings are added to the configuration file for each virtual machine wanting to share this disk — you need to point each virtual machine to this disk.

Sharing a Disk on the scsi0 Bus

VMware does not recommend sharing a disk on SCSI bus 0. This bus is usually used for the boot disk. If you share the boot disk, you run the risk of corrupting it, as the boot program is not aware that the disk is being shared and can write to the disk regardless of whether or not it is being shared. It is far more secure to use SCSI reservation on a data disk located on a different bus.

Issues to Consider When Sharing Disks

- Do **not** try to share a disk among multiple running virtual machines that are not collocated on the **same** host. The disk file itself may be located remotely, but the virtual machines must be running together on the same GSX Server host. If you try to share a disk among virtual machines located on different hosts, you could encounter the same unpredictable results you would expect to find if you disabled disk locking.
- If only one running virtual machine is using a given disk, and it is running applications that do not use SCSI reservation, then the disk's performance might be degraded slightly.
- At this time, if one virtual machine does **not** have SCSI reservation enabled for its virtual disk, but another virtual machine **does** have SCSI reservation enabled for the same virtual disk, GSX Server **does** allow the disk to be shared. However, any virtual machine not configured for SCSI reservation that tries to access this disk concurrently can cause corruption or data loss on the shared disk. VMware recommends you take care when sharing disks.
- If you need to shrink or defragment the virtual disk (provided it is not a preallocated virtual disk or a physical disk), first disable SCSI reservations and make sure the virtual disk is not being used by any other virtual machine. To disable SCSI reservation for a virtual machine, open the configuration file and comment out or remove the `scsi[n].sharedBus = "virtual"` line and make sure the `disk.locking` line is set to `"true"`.
- If your host abnormally terminates or another action occurs that may require you to repair the preallocated virtual disk, power on the virtual machine using the virtual disk and repair the disk in one virtual machine before using it in another virtual machine. Doing these steps ensures that only one copy of the disk checker runs at one time.
- In a Windows virtual machine, some disk errors are recorded in the Windows event log in normal operation. These error messages have a format similar to `"The driver detected a controller error on \Device\Scsi\BusLogic3"`

The errors should appear in the log periodically only on the passive node of the cluster and should also appear when the passive node is taking over during a failover. The errors are logged because the active node of the cluster has reserved the shared virtual disk. The passive node periodically probes the shared disk and receives a SCSI reservation conflict error.

Overview of Clustering with GSX Server

GSX Server clustering capabilities are ideally suited for development, testing and training applications.

Note: Always rigorously test and review your cluster before deploying it in a production environment.

This section includes:

- [Applications That Can Use Clustering on page 198](#)
- [Clustering Software in Virtual Machines on page 198](#)

Clustering is providing a service via a group of servers to get high availability, scalability or both.

For example:

- In a Web server cluster where the Web site serves static content, a gateway distributes requests to all nodes according to load. The gateway also redirects requests to remaining nodes if one crashes.

This configuration increases availability and performance over a single-machine approach. Network Load Balancing in Windows 2000 provides such a service.

- In a more complex cluster, a single node might serve a database. If that node crashes, it must restart the database on another node. The database application knows how to recover from a crash. In normal operation, other nodes run other applications.

Microsoft Cluster Service and Veritas Cluster Service provide such a service.

In a typical virtual machine cluster:

- Each virtual machine is one node in the cluster.
- Disks are shared between nodes.

Shared disks are needed if the application uses dynamic data as mail servers or database servers do.

When using virtual disks, you must preallocate the disk space at the time you create the virtual disk.

- There are extra network connections between nodes for monitoring heartbeat status.
- There is a method for redirecting incoming requests.

Applications That Can Use Clustering

To take advantage of clustering services, applications need to be clustering-aware. Such applications can be stateless, such as Web servers and VPN servers. Clustering-aware applications often include built-in recovery features, like those in database servers, mail servers, file servers or print servers.

Clustering Software in Virtual Machines

Available clustering software includes:

- Microsoft Clustering Service (MSCS) — which provides fail-over support for two to four-node clusters for applications such as databases, file servers and mail servers.
- Microsoft Network Load Balancing (NLB) — that balances the load of incoming IP traffic across a cluster of up to 32 nodes for applications such as Web servers and terminal services.
- Veritas Clustering Service (VCS).
- Novell Clustering Services.

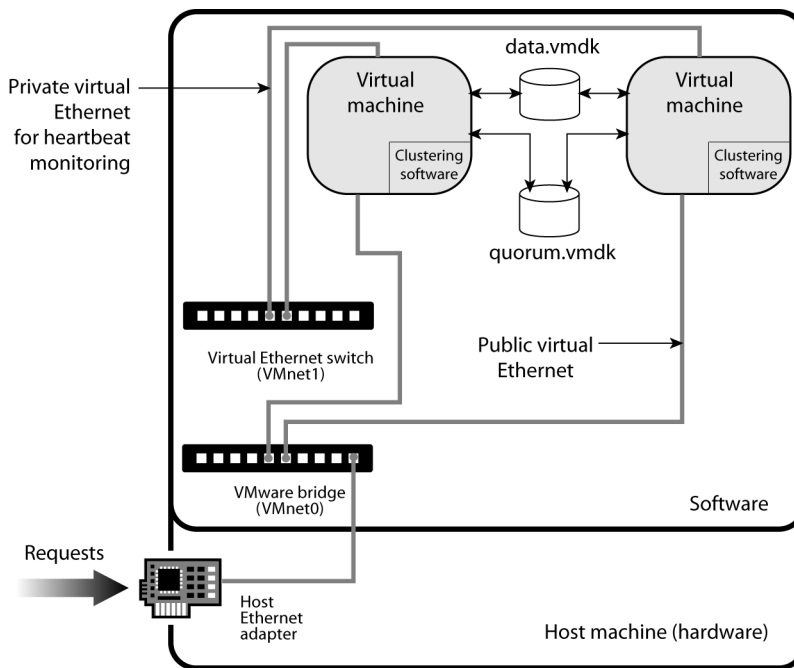
Note: These clustering services are tested and supported by VMware only with Windows host operating systems.

Creating a Cluster in a Box

With GSX Server, you can create a simple cluster in a box to help mitigate the effects of software crashes or administrative problems.

This type of cluster:

- Consists of multiple virtual machines (nodes) on a single physical machine.
- Supports shared disks without any shared SCSI hardware.
- Supports a heartbeat network without an extra network adapter.



A two-node cluster on a single physical machine.

The following sections describe how to set up a cluster in a box:

- [Configuring Virtual Machines for Cluster in a Box on page 200](#)
- [Creating a Two-Node Cluster with Microsoft Clustering Services on a Single GSX Server Computer on page 201](#)
- [Creating the First Node's Base Virtual Machine on page 201](#)

- [Installing the Guest Operating System in the First Virtual Machine \(Node\) on page 203](#)
- [Cloning the First Cluster Node on page 203](#)
- [Creating the Second Node in the Cluster from the Clone of the First Node on page 204](#)
- [Installing Microsoft Clustering Services on the Cluster Nodes on page 205](#)

Configuring Virtual Machines for Cluster in a Box

To create a set of clustered virtual machines (a cluster in a box), configure each of them with the following:

- A primary virtual SCSI host adapter with one SCSI virtual disk.
- Two virtual network adapters:
 - A public network adapter bridged to a physical adapter either using VMnet0, or VMnet2-8 as configured in the virtual machine settings editor of the GSX Server machine.
 - A private network adapter connected to VMnet1 (host-only), or another physical adapter (VMnet2 through VMnet8). This is the network adapter that the clustering service uses to monitor the heartbeat between nodes. This device selection must match in all virtual machines in a cluster set.
- The remaining default virtual machine devices (such as the CD-ROM drive and the floppy disk drive).

In addition to the above devices, the following are required for shared storage:

- A secondary virtual SCSI host adapter.
- One or more preallocated virtual disks that are shared, attached to the secondary SCSI host adapter.

Please note the following about virtual PCI slots in the virtual machines:

- Each virtual machine by default has six PCI slots available.
- This configuration (two network adapters and two SCSI host bus adapters) uses four of these slots.
- **One** more PCI slot **is** available for a third network adapter if needed.

(The sixth slot is used by the virtual display adapter.)

Creating a Two-Node Cluster with Microsoft Clustering Services on a Single GSX Server Computer

This procedure creates a two-node cluster using Microsoft Clustering Services on a single GSX Server computer using the following:

- SQL1 = host name of node 1 of the cluster
- SQL2 = host name of node 2 of the cluster
- SQLCLUSTER = public host name of the cluster

Creating the First Node's Base Virtual Machine

The following steps describe how to create the base virtual machine that serves as the first node in the cluster (and as a template for the additional node), and how to create the two preallocated virtual disks that are shared among the virtual machines in the cluster.

Note: The virtual disks used to store the operating system and clustering software for each virtual machine (node) in the cluster do not have to be preallocated virtual disks.

1. Log on to your GSX Server host as the user who will own the virtual machine.
2. Launch a VMware Virtual Machine Console and create a new virtual machine (for information on creating a new virtual machine, see [Creating a New Virtual Machine](#) in the *VMware GSX Server Virtual Machine Guide*). Follow the Custom path. Choose the settings you want (for example, the size of the virtual disk or the amount of memory), but make sure you specify
 - Windows 2000 Advanced Server as the guest operating system.
 - SQL1 as the virtual machine name.
 - The virtual machine directory as `d:\cluster\SQL1` (on a Windows host) or `/home/cluster/SQL1` (on a Linux host).
 - Bridged networking for the virtual machine.
 - SQL1 as the disk file name.
3. Open the virtual machine settings editor. Choose **VM > Settings**.
4. Add a new network adapter that uses either another external adapter or the VMnet1 host-only adapter. (For complete isolation from the host, you may also use any unused virtual Ethernet switch, typically VMnet2 through VMnet7.) For information, see [Adding and Modifying Virtual Network Adapters](#) in the *VMware GSX Server Virtual Machine Guide*.

This adapter is used as the virtual private Ethernet connection for heartbeat monitoring.

5. Add the two virtual disks that are to be shared:
 - A shared data disk (call it `data.vmdk`, for example)
 - A shared quorum disk (call it `quorum.vmdk`, for example) to store transactions before they are committed to the data disk

For information, see [Adding Virtual Disks to a Virtual Machine](#) in the *VMware GSX Server Virtual Machine Guide*.

6. Click **OK** to save your changes and close the virtual machine settings editor.
7. Using a text editor, manually edit the configuration file
`d:\cluster\SQL1\SQL1.vmx` (on a Windows host) or
`/home/cluster/SQL1/SQL1.vmx` (on a Linux host).
8. Add the following lines to the bottom of the configuration file:


```
scsi1.sharedBus = virtual
disk.locking = "false"
```

This enables SCSI reservation, which is described in more detail in the section [Using SCSI Reservation to Share SCSI Disks with Virtual Machines](#) on page 192.

You are finished creating the virtual machine for the first node in your cluster. The next step is to install a guest operating system in the virtual machine.

Installing the Guest Operating System in the First Virtual Machine (Node)

Follow these steps to install Windows 2000 Advanced Server in the virtual machine that is the first node of your cluster:

1. Insert the Windows 2000 Advanced Server CD in the CD-ROM drive.
2. Connect to the virtual machine with a console.
3. Log in as the user who created the virtual machine, as root or as the Administrator.
4. Click **Power On**.
5. Install Windows 2000 Advanced Server on the disk connected to `scsi0`.
6. Accept all of the default options during the installation.

Note: Do not install the clustering services at this time.

7. When the installation is complete, install VMware Tools in the guest operating system. See [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide*.
8. Remove the Windows 2000 Advanced Server CD from the CD-ROM drive.

You are finished installing the guest operating system. The next step is to clone the virtual machine. (Later, you create the second cluster node using the clone.)

Cloning the First Cluster Node

Follow these steps to clone the first virtual machine node:

1. Run `sysprep.exe`, which is available on the Windows 2000 CD in the file `\support\tools\deploy.cab` (or from the Microsoft Web site).
The `sysprep.exe` utility removes the security ID assigned to the guest operating system, resets the machine information and resets the TCP/IP network configuration.
2. Shut down the guest operating system and power off the virtual machine.
3. Create a directory named `SQL2` under the `cluster` directory.
4. Copy the `SQL1*.vmdk` files into this directory.
5. Change the file names to `SQL2*.vmdk`.

You are finished cloning the first node. You are now ready to create the second node in the cluster using the clone.

Creating the Second Node in the Cluster from the Clone of the First Node

Follow these steps to create the second node in the cluster using the clone of the first node:

1. Log on to your GSX Server host as the user who will own the virtual machine.
2. Launch a VMware Virtual Machine Console and create a new virtual machine (for information on creating a new virtual machine, see [Creating a New Virtual Machine](#) in the *VMware GSX Server Virtual Machine Guide*). Choose the settings you want (for example, the size of the virtual disk or the amount of memory), but make sure you specify:
 - Windows 2000 Advanced Server as the guest operating system.
 - SQL2 as the virtual machine name.
 - The virtual machine directory as `d:\cluster\SQL2` (on a Windows host) or `/home/cluster/SQL2` (on a Linux host).
 - Bridged networking for the virtual machine.
 - To use an existing virtual disk, click **Browse** and select `SQL2.vmdk`.
3. Open the virtual machine settings editor. Choose **VM > Settings**.
4. Add a new network adapter that uses either another external adapter or the VMnet1 host-only adapter. For information, see [Adding and Modifying Virtual Network Adapters](#) in the *VMware GSX Server Virtual Machine Guide*.
5. Add the two virtual disks (`quorum.vmdk` and `data.vmdk`) you previously created. For information, see [Adding Virtual Disks to a Virtual Machine](#) in the *VMware GSX Server Virtual Machine Guide*. Make sure you choose to **Use an existing virtual disk** and browse to `quorum.vmdk` and `data.vmdk`.
6. Click **OK** to save your settings and close the virtual machine settings editor.
7. Using a text editor, manually edit the configuration file `d:\cluster\SQL2\SQL2.vmx` (on a Windows host) or `/home/cluster/SQL2/SQL2.vmx` (on a Linux host).
8. Add the following lines to the bottom of the configuration file:


```
scsi1.sharedBus = virtual
disk.locking = "false"
```

This enables SCSI reservation, which is described in more detail in the section [Using SCSI Reservation to Share SCSI Disks with Virtual Machines on page 192](#).
9. Connect to the VMware Management Interface (`https://<hostname>:8333`) and review the Status Monitor page.

The management interface should list both virtual machines and show them powered off.

You are finished creating the second node.

Now that you have virtual machines for both nodes in your two-node cluster, you are ready to install the clustering services software.

Installing Microsoft Clustering Services on the Cluster Nodes

Follow these steps to install Microsoft Clustering Services on the first node of your cluster:

1. Start the node 1 virtual machine.
2. Follow the Windows 2000 Advanced Server setup prompts to enter
 - The Windows 2000 Advanced Server serial number.
 - The host name (SQL1).
 - The IP addresses of the public and private network adapters.

Note: For the public network adapter, enter an IP address that belongs to the physical network. For the private IP address, you may use an address like 192.168.x.x with a class C subnet mask (255.255.255.0).

3. At the end of the process, Windows automatically reboots.
4. Start the Disk Management tool and change both shared disks to **Basic** disks.
5. Format both shared virtual disks with NTFS if they are not already formatted.
6. Assign the first shared disk to **Q:** (quorum) and the second disk to **R:** (data).

If you have joined this virtual machine to an existing Active Directory domain, skip to step 11.

7. Run `dcpromo.exe` from the command prompt. This starts the Active Directory Wizard.
8. Set up the current machine as a domain controller. For the domain name, use something similar to `<vmcluster>.<domain.com>` where `<domain.com>` is your DNS domain and `<vmcluster>` is your Active Directory domain.

You can set up this node as a new domain tree or a new domain forest, or join it to an existing domain tree or forest.

9. Make sure the DNS server is installed.
10. Set the domain permissions as mixed mode unless you plan otherwise.

11. To add a cluster services account in the domain, go to **Programs > Administrative Tools > Active Directory Users and Computers**.
12. Add a cluster service account named `cluster`:
 - Enter the user's password.
 - Check the **User cannot change password** check box.
 - Check the **Password never expires** check box.
13. Insert the Windows 2000 Advanced Server CD in the CD-ROM drive.
14. Choose **Control Panel > Add/Remove Programs**.
15. Select **Add/Remove Windows Components**.
16. Check the **Cluster Service** component.
17. Click **Next** and follow the prompts to install the service.
18. As you configure the cluster service, choose **Form a New Cluster**.
19. Specify `SQLCLUSTER` as the cluster name.
20. Specify the cluster service account created in step 12.
21. Specify that both shared disks should be managed by the cluster service.
22. Indicate the shared disk (`Q :`) to be the quorum disk.
23. Specify which network adapter is public and which is private.
24. Specify the cluster IP address. This is the address that represents the cluster. It must be on the same network as the physical Ethernet device.
25. Stop the cluster service on the local node (node 1) so that the second virtual machine (node 2) can access the shared disks.
 - From Cluster Manager, right-click the node name.
 - Select **Stop Cluster Service**.

You are finished installing Microsoft Clustering Services on the first node. The steps to install the software on the second node are similar.

1. Start the node 2 virtual machine.
2. Repeat step 2 and step 3 in the procedure for the first node.
3. Start the Disk Management tool and assign the first shared disk to `Q :` (quorum) and the second disk to `R :` (data).
4. Start `dcpromo.exe` and add this virtual machine as a domain controller in the same domain created in step 8 for the first node, or add it to an existing domain.

Note: The setup in node 2 must match the setup in node 1, which you specified in step 8 for node 1.

5. In the node 1 virtual machine, start the cluster service.
 - From Cluster Manager, right-click the node name.
 - Select **Start Cluster Service**.
6. In the node 2 virtual machine, repeat step 14 through step 24 in [Installing Microsoft Clustering Services on the Cluster Nodes on page 205](#), **with one exception:** in step 18, select **Join a Cluster**.

You are now finished configuring the cluster.

Using Network Load Balancing with GSX Server

This section covers procedures for creating a multinode Network Load Balancing cluster using nodes running in virtual machines. These virtual machines can be located on one or more GSX Server computers.

Overview of Network Load Balancing Clusters

Network Load Balancing is a Windows 2000 Advanced Server feature. Using Network Load Balancing to build a server cluster:

- You can enhance the availability of Internet server programs, such as those used on these types of servers:
 - Web
 - Proxy
 - Domain name service (DNS)
 - FTP
 - Virtual private network (VPN)
 - Streaming media servers
 - Terminal services
- You can scale your server's performance.
- You can create the cluster with virtual machines on the same physical server or with virtual machines on multiple physical servers (all running GSX Server).
- You can configure up to 32 nodes in the cluster.

Creating a Multinode Network Load Balancing Cluster

The next sections describe how to create a multinode Network Load Balancing cluster.

Creating the First Node's Base Virtual Machine

Follow these steps to create a base virtual machine that is the first node in your Network Load Balancing cluster:

1. Log on to your GSX Server host as the user who will own the virtual machine.
2. Launch a VMware Virtual Machine Console and create a new virtual machine (for information on creating a new virtual machine, see [Creating a New Virtual Machine](#) in the *VMware GSX Server Virtual Machine Guide*). Choose the settings you want (for example, the size of the virtual disk or the amount of memory), but make sure you specify
 - Windows 2000 Advanced Server as the guest operating system.
 - NLB1 as the virtual machine name.
 - The virtual machine directory as `d:\cluster\nlb1` (on a Windows host) or `/home/cluster/nlb1` (on a Linux host).
 - Bridged networking for the virtual machine.
 - `nlb1` as the disk file name.
3. Connect to this virtual machine with the VMware Virtual Machine Console and choose **VM > Settings**.
4. Add a second networking device, binding it to another physical NIC or to the host-only network.

You are finished creating the first virtual machine (node) in the cluster. The next step is to install a guest operating system in the virtual machine.

Installing the Guest Operating System in the First Virtual Machine (Node)

Follow these steps to install Windows 2000 Advanced Server in the virtual machine that is the first node in your load balancing cluster:

1. Insert the Windows 2000 Advanced Server CD in the CD-ROM drive.
2. Connect to the virtual machine with a console.
3. Log in using the user account that created the virtual machine, or log in as root or the Administrator.
4. Click **Power On**.
5. Install Windows 2000 Advanced Server on the disk connected to `scsi0`.

6. Accept all the default options during the installation. You can install the applications at this time. Network Load Balancing is installed by default.
7. When the installation is complete, install VMware Tools in the guest operating system. See [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide*.
8. Remove the Windows 2000 Advanced Server CD from the CD-ROM drive.

You are finished creating the first cluster node. You may now clone that node for use in creating other nodes.

Cloning the First Cluster Node

Follow these steps to clone the first cluster node for use in creating the other nodes in the cluster, either on the same physical server or on other machines running GSX Server:

1. Run `sysprep.exe`, which is available on the Windows 2000 CD in the file `\support\tools\deploy.cab` or from the Microsoft Web site.
The `sysprep.exe` utility removes the security ID assigned to the guest operating system, resets the machine information and resets the TCP/IP network configuration.
2. Shut down the guest operating system and power off the virtual machine.
3. Create a directory `n1b2` under the cluster directory, either on the local server or on different machines running GSX Server.
4. Copy the `n1b1*.vmdk` files into this directory.
5. Change the file names to `n1b<n>*.vmdk`. (where `<n>` is the Network Load Balancing node number.

Repeat step 3 through step 5 for each additional node you wish to create, either on the same physical server, or on additional machines running GSX Server. You may configure up to 32 nodes with Network Load Balancing.

When you are finished making clones of the first node, you are ready to create additional nodes from the clones.

Creating the Additional Nodes in the Network Load Balancing Cluster

Follow these steps for each of the additional nodes you wish to create (up to 32 nodes) in the Network Load Balancing cluster:

1. Log on to your GSX Server host as the user who will own the virtual machine.
2. Launch a VMware Virtual Machine Console and create a new virtual machine (for information on creating a new virtual machine, see [Creating a New Virtual](#)

[Machine](#) in the *VMware GSX Server Virtual Machine Guide*). Choose the settings you want (for example, the size of the virtual disk or the amount of memory), except you should specify

- Windows 2000 Advanced Server as the guest operating system.
- `n1b2` as the virtual machine name.

Note: For each additional node, use the name of that node instead of `n1b2`.

- The virtual machine directory as `d:\VMware\cluster\n1b2` (on a Windows host) or `/home/cluster/n1b2` (on a Linux host).
 - To use an existing virtual disk. Click **Browse** and select `n1b2.vmdk`.
 - Bridged networking for the virtual machine.
3. Connect to this virtual machine with the VMware Virtual Machine Console and choose **VM > Settings**.
 4. Add a second networking device, binding it to another physical NIC or to the host-only network. For information, see [Adding and Modifying Virtual Network Adapters](#) in the *VMware GSX Server Virtual Machine Guide*.
 5. Close the console and connect to the VMware Management Interface (`https://<hostname>:8333`) and review the Status Monitor page.
The management interface should list both virtual machines and show them powered off.

After you have finished creating the additional nodes, you are ready to configure the cluster.

Configuring the Network Load Balancing Cluster

You can cluster up to 32 nodes using Network Load Balancing.

To configure the cluster, follow these steps for each node that joins the cluster:

1. Connect to the first node virtual machine with the VMware Virtual Machine Console.
2. Power on the virtual machine.
3. Follow the Windows 2000 Server mini-setup prompts to enter the following:
 - The Windows 2000 Advanced Server serial number
 - The host name
 - IP addresses for that host
4. At the end of the process, Windows automatically reboots.

5. Log on to the Windows 2000 Advanced Server virtual machine as the Administrator user.
6. Open **Network and Dial-up Connections**.
7. Right-click the local area connection on which you want to install Network Load Balancing and choose **Properties**.

The Local Area Connection Properties dialog box appears.

8. Under **Components checked are used by this connection**, select the **Network Load Balancing** check box.
9. Click **Properties**.
10. On the **Cluster Parameters** tab, configure cluster operations using these parameters:

- **Primary IP Address:** This is the address for the cluster as a whole. Clients use this address to access the cluster.
- **Subnet Mask:** This is the subnet mask of the network to which the above address belongs.
- **Multicast:** Leave this unchecked, unless your virtual machine was configured with a single network adapter.

Note: All members of the cluster must use the same setting for the **Multicast** option.

Refer to Network Load Balancing online Help for the remaining options.

11. When you finish with the cluster parameters, click **OK** to return to the Local Area Connection Properties dialog box.
12. Click **OK** to return to the Local Area Connection Status dialog box.
13. Right-click the local area connection on which Network Load Balancing is to be installed, and select **Properties**.
14. Click **Internet Protocol (TCP/IP)**, then click **Properties**.
15. Set up TCP/IP for Network Load Balancing.

For more information and links to procedures for setting up TCP/IP for Network Load Balancing on single and multiple network adapters, see Related Topics in the Network Load Balancing online Help.

Note: You must add the cluster's primary IP address to the list of IP addresses bound to the adapter.

Repeat these steps on each host to be used in your Network Load Balancing cluster.

Creating Two-Node Clusters Using Novell Clustering Services

This section describes procedures for creating a two-node cluster using Novell Clustering Services on a single VMware GSX Server system using the following:

- Cluster1: host name of node 1 of the cluster
- Cluster2: host name of node 2 of the cluster

Creating the First Node's Base Virtual Machine

The following steps describe how to create the base virtual machine that serves as the first node in the cluster, as well as how to create the two preallocated virtual disks that are shared among the virtual machines in the cluster. You can install Novell NetWare 6.0 or 6.5 in a virtual machine using the standard NetWare 6.0 or 6.5 CD-ROM. VMware recommends you install NetWare 6.0 on a host with at least 384MB of memory; NetWare 6.5 must be installed on a host with 512MB of memory.

Creating and Configuring the NetWare Virtual Machine

Note: The virtual disks used to store the operating system and clustering software for each virtual machine (node) in the cluster do not have to be preallocated virtual disks.

1. Log on to your GSX Server host as the user who will own the virtual machine.
2. Launch a VMware Virtual Machine Console and create a new virtual machine (for information on creating a new virtual machine, see [Creating a New Virtual Machine](#) in the *VMware GSX Server Virtual Machine Guide*). Choose the settings you want (for example, the size of the virtual disk or the amount of memory), but make sure you specify:
 - Netware 6 as the guest operating system.
 - Cluster1 as the virtual machine name.
 - The virtual machine directory as `D:\Netware6\Cluster1` (on a Windows host) or `/home/Netware/Cluster1` (on a Linux host).
 - Bridged networking for the virtual machine.

You are finished creating the virtual machine for the first node in your cluster. The next step is to create the second node in your cluster. Then, for each node, install the guest operating system and VMware Tools, which includes the CPU

idler program. See the NetWare installation notes in the *VMware Guest Operating System Installation Guide* on the console Help menu for details.

Creating the Second Node in the Cluster

Next, create the second node of the cluster by following the same procedure for creating the first node listed above with the following changes:

- Use Cluster2 as the virtual machine name.
- The virtual machine directory as `D:\Netware6\Cluster2` (on a Windows host) or `/home/Netware/Cluster2` (on a Linux host).

Installing the Guest Operating System and VMware Tools

To install NetWare 6.0 or 6.5 in a virtual machine, complete the steps in the *VMware Guest Operating System Installation Guide*. Make sure you follow the instructions for bridged networking.

After you finish the installation, install VMware Tools, which installs and loads the CPU idler program. For details, see [Installing VMware Tools](#) in the *VMware GSX Server Virtual Machine Guide*.

Installing VMware Tools also installs and loads the CPU idler program. NetWare servers do not idle the CPU when the operating system is idle. As a result, a virtual machine takes CPU time from the host regardless of whether the NetWare server software is idle or busy. To prevent unnecessary slowdowns, VMware recommends that after you install VMware Tools, you keep the NetWare CPU idle program loaded.

Be sure to read the known issues for NetWare 6.0 or 6.5 in the installation guidelines.

Adding the Shared Disks to Both Virtual Machines

Follow the procedure outlined in [Adding Virtual Disks to a Virtual Machine](#) in the *VMware GSX Server Virtual Machine Guide* to create and add two shared preallocated virtual disks to the first node (called Cluster1). These disks are shared between both nodes and include:

- A shared data disk (call it `data.vmdk`, for example).
- A shared quorum disk (call it `quorum.vmdk`, for example).

Note: Use the Advanced option when adding the preallocated virtual disks from the virtual machine settings editor to select SCSI virtual device nodes for the disks.

After you finish creating the virtual disks, add them to the second node by completing the following steps.

1. Open the virtual machine settings editor for the node 2 virtual machine (called Cluster2). Choose **VM > Settings**.
2. Add the two virtual disks that are to be shared. Instead of creating new virtual disks, use the existing virtual disks created for node 1 (called Cluster1).
3. Click **OK** to save your changes and close the virtual machine settings editor.
4. For the virtual machine named Cluster1, use a text editor to manually edit the configuration file. This file is `D:\Netware6\Cluster1\Cluster1.vmx` on a Windows host or `/home/Netware/Cluster1/Cluster1.vmx` on a Linux host.
5. For the virtual machine named Cluster2, use a text editor to manually edit the configuration file. This file is `D:\Netware6\Cluster2\Cluster2.vmx` on a Windows host or `/home/Netware/Cluster2/Cluster2.vmx` on a Linux host.
6. Add the following lines to the bottom of each configuration file:
`scsi0.sharedBus = "virtual"`
`disk.locking = "false"`

Note: The default virtual disk type is IDE for the base virtual machine's virtual disk created in [Creating the First Node's Base Virtual Machine on page 213](#). If you are using SCSI virtual disks for the base virtual machine instead, the configuration file options for the shared bus are:

```
scsi1.present = "true" (If this line already exists, do not add it again.)
scsi1.sharedBus = "virtual"
disk.locking = "false"
```

These settings are necessary because your base virtual machine's virtual disk is attached to `scsi0` and you **must** have a separate virtual SCSI card for attaching the shared disks. The settings enable SCSI reservation for `scsi1`, which is described in more detail in [Using SCSI Reservation to Share SCSI Disks with Virtual Machines on page 192](#).

Installing Novell Clustering Services on the Cluster Nodes

Complete the following steps to install Novell Clustering Services in each virtual machine.

1. Power on the first node virtual machine (Cluster1).
2. Boot into DOS by pressing the **F5** key to bypass running the startup files.
3. Insert the driver floppy disk in the host's floppy drive.
4. Copy the drivers to the `c:\nwserver` directory.

5. Remove the driver floppy disk in the host's floppy drive.
6. Reboot the virtual machine.
7. The server should be able to recognize the shared disks. You may verify that by running `List Devices`.

Repeat the above steps for the node 2 virtual machine (Cluster2).

Now you are ready to install the Novell Clustering Services (NCS) as you would normally on two physical machines. Please refer to the NetWare 6.0 or 6.5 product documentation for details.

Glossary

Bridged networking — A type of network connection between a virtual machine and the rest of the world. Under bridged networking, a virtual machine appears as an additional computer on the same physical Ethernet network as the host.

See also Host-only networking.

Configuration — See Virtual machine configuration file.

Console — See VMware Virtual Machine Console.

Custom networking — Any type of network connection between virtual machines and the host that does not use the default bridged, host-only or network address translation (NAT) networking configurations. For instance, different virtual machines can be connected to the host by separate networks or connected to each other and not to the host. Any network topology is possible.

Existing partition — A partition on a physical disk in the host machine.

See also Physical disk.

Full screen mode — A display mode in which the virtual machine's display fills the entire screen.

See also Quick switch mode.

Guest operating system — An operating system that runs inside a virtual machine.

See also Host operating system.

Headless — A program or application that runs in the background without any interface connected to it. A running virtual machine that has no consoles connected to it is running headless.

Host-only networking — A type of network connection between a virtual machine and the host. Under host-only networking, a virtual machine is connected to the host on a private network, which normally is not visible outside the host. Multiple virtual machines configured with host-only networking on the same host are on the same network.

See also Bridged networking, Custom networking and Network address translation.

Host computer — The physical computer on which the GSX Server software is installed. It hosts the GSX Server virtual machines.

Host operating system — An operating system that runs on the host machine. See also Guest operating system.

Independent disk — Independent disks are not affected by snapshots.

Inventory — A list in the left panel of the console window that shows the names of virtual machines that a user has added to the list. The Inventory makes it easy to launch a virtual machine or to connect to the virtual machine's configuration file in order to make changes in the virtual machine settings.

Network address translation (NAT) — A type of network connection that allows you to connect your virtual machines to an external network when you have only one IP network address, and that address is used by the host computer. If you use NAT, your virtual machine does not have its own IP address on the external network. Instead, a separate private network is set up on the host computer. Your virtual machine gets an address on that network from the VMware virtual DHCP server. The VMware NAT device passes network data between one or more virtual machines and the external network. It identifies incoming data packets intended for each virtual machine and sends them to the correct destination.

See also Bridged networking, Custom networking and Host-only networking.

New Virtual Machine Wizard — A point-and-click interface for convenient, easy creation of a virtual machine configuration. To launch it, choose **File > New Virtual Machine**. It prompts you for information, suggesting default values in most cases. It creates files that define the virtual machine, including a virtual machine configuration

file and (optionally) a virtual disk or physical disk file.

See also Virtual Machine Settings Editor.

Nonpersistent mode — If you configure a virtual disk as an independent disk in nonpersistent mode, all disk writes issued by software running inside a virtual machine with a disk in nonpersistent mode appear to be written to disk but are in fact discarded after the virtual machine is powered off. As a result, a virtual disk or physical disk in independent-nonpersistent mode is not modified by GSX Server.

See also Independent disk, Persistent mode

Persistent mode — If you configure a virtual disk as an independent disk in persistent mode, all disk writes issued by software running inside a virtual machine are immediately and permanently written to a virtual disk in persistent mode. As a result, a virtual disk or physical disk in independent-persistent mode behaves like a conventional disk drive on a physical computer.

See also Independent disk, Nonpersistent mode

Physical disk — A hard disk in a virtual machine that is mapped to a physical disk drive or partition on the host machine. A virtual machine's disk can be stored as a file on the host file system (see Virtual disk) or on a local hard disk. When a virtual machine is configured to use a physical disk, GSX Server directly accesses the local disk or partition as a raw device (not as a file on a file system). It is possible to boot a previously installed operating system on an existing partition within a virtual machine environment. The only limitation is that the existing partition must reside on a local IDE or SCSI drive.

See also Virtual disk.

Preallocated disk — A type of virtual disk where all disk space for the virtual machine is allocated at the time the disk is created. This is the default type of virtual disk created by GSX Server.

Quick switch mode — A display mode in which the virtual machine's display fills most of the screen. In this mode, tabs at the top of the screen allow you to switch quickly from one running virtual machine to another.

See also Full screen mode.

Redo log — The file that stores the changes made to a disk in independent-nonpersistent mode. The redo-log file is deleted when you power off or reset the virtual machine without writing any changes to the disk.

Resume — Return a virtual machine to operation from its suspended state. When you resume a suspended virtual machine, all applications are in the same state they were when the virtual machine was suspended.

See also Suspend.

Shrink — The method to reclaim unused space in a virtual disk. If there is empty space in the disk, shrinking reduces the amount of space the virtual disk occupies on the host drive. Shrinking virtual disks is a convenient way to convert an older virtual disk (created by GSX Server 1 for example) to the `.vmdk` format supported by GSX Server 3. You cannot shrink preallocated virtual disks or physical disks.

Snapshot — A snapshot preserves the virtual machine just as it was when you took the snapshot — the state of the data on all the virtual machine's disks and whether the virtual machine was powered on, powered off or suspended. GSX Server lets you take a snapshot of a virtual machine at any time and revert to that snapshot at any time. You can take a snapshot when a virtual machine is powered on, powered off or suspended.

Supported partition — A virtual disk partition that VMware Tools can prepare for shrinking, such as one of the drives that comprise the virtual hard disk. You can choose to not prepare certain partitions for shrinking.
See also Shrink.

Suspend — Save the current state of a running virtual machine. To return a suspended virtual machine to operation, use the resume feature.
See also Resume.

Unsupported partition — A virtual disk partition that VMware Tools cannot prepare for shrinking. Unsupported partitions include read-only drive partitions, partitions on remote devices and partitions on removable devices such as floppy drives or CD-ROM drives.
See also Shrink.

Virtual disk — A virtual disk is a file or set of files that appears as a physical disk drive to a guest operating system. These files can be on the host machine or on a remote file system. When you configure a virtual machine with a virtual disk, you can install a new operating system into the disk file without the need to repartition a physical disk or reboot the host.
See also Physical disk.

Virtual machine — A virtualized x86 PC environment in which a guest operating system and associated application software can run. Multiple virtual machines can operate on the same host machine concurrently.

Virtual machine configuration — The specification of what virtual devices (disks, memory size, etc.) are present in a virtual machine and how they are mapped to host files and devices.

Virtual machine configuration file — A file containing a virtual machine configuration. It is created when you create the virtual machine. It is used by GSX Server to identify and run a specific virtual machine.

Virtual Machine Settings Editor — A point-and-click control panel used to view and modify a virtual machine's settings. You launch it by choosing **VM > Settings**. See also New Virtual Machine Wizard.

Virtual Network Editor — A point-and-click editor used to view and modify the networking settings for the virtual networks created by GSX Server. You launch by choosing **Host > Virtual Network Settings**.

VMware Authorization Service — The service VMware GSX Server employs to authenticate users. The process is called `vmware-authd` on Linux hosts.

VMware guest operating system service — One of the components installed with VMware Tools that performs various duties in the guest operating system, like executing commands in the virtual machine, gracefully shutting down and resetting a virtual machine, sending a heartbeat to VMware GSX Server, synchronizing the time of the guest operating system with the host operating system and passing strings from the host operating system to the guest operating system.

VMware Management Interface — A browser-based tool that allows you to control (start, suspend, resume, reset and stop), configure and monitor virtual machines and the server on which they run.

VMware Registration Service — The service VMware GSX Server employs for managing connections to virtual machines and the management interface. This process is known as `vmware-serverd` on Linux hosts.

VMware Tools — A suite of utilities and drivers that enhances the performance and functionality of your guest operating system. Key features of VMware Tools include some or all of the following, depending on your guest operating system: an SVGA driver, a mouse driver, the VMware guest operating system service, the VMware Tools control panel and support for such features as shrinking virtual disks, time synchronization with the host, VMware Tools scripts and connecting and disconnecting devices while the virtual machine is running.

VMware Virtual Machine Console — An interface to a virtual machine that provides access to one or more virtual machines on the local host or a remote host running GSX Server. You can view the virtual machine's display to run programs within it or modify guest operating system settings. In addition, you can change the virtual machine's configuration, install the guest operating system or run the virtual machine in full screen mode.

Index

Symbols

.vmdk 163, 166, 169

A

Apache
and management interface 141

Authentication
Linux hosts 111
Windows hosts 108

Authentication daemon
Linux host 111

B

Backup
GSX Server host 120

Backup agent
in virtual machine 119
on host 119

BIOS
provided in virtual machine 26

Bridged networking
defined 217

Browser
configuring on Linux host 63

BSD
supported guest operating systems
30

C

CD
CD-ROM image file 26

Clustering 197
applications 198
cluster in a box 199
configuring virtual machines 200
multinode Network Load Balancing
cluster 209
Network Load Balancing 208
Novell Clustering Services 213
software 198
two-node cluster 213
two-node clusters 201

Configuration
virtual machine 220

Configure
after Linux kernel upgrade 55

memory size 185
Web browser on Linux host 63

Core files 33

CPU
host requirement 19
provided in virtual machine 26

Ctrl-Alt-Delete
in virtual machines 153

D

Debugging information
enable for virtual machine 134

Default directories 42, 53

Devices
provided in virtual machine 26

Disks
available in virtual machine 26
existing partition 217
physical 219
virtual 220

Drives
See Disks

E

Encrypting remote sessions 112

Event viewer 117

F

Floppy
drives in virtual machine 27
image file 27

FreeBSD
supported guest operating systems
30

Full screen mode
defined 217

G

Generic SCSI
virtual machine backup 119

Graphics
support in virtual machine 26

GSX Server
global preferences 154
software updates 150
user preferences 149

- GSX Server host
 - configuring 143
 - default virtual machine directory 154
 - securing connections with SSL 144
- Guest operating system
 - defined 13, 218
 - supported 29

H

- Headless 218
- Heartbeat
 - virtual machine 128
- Help
 - configuring Web browser for, on Linux host 63
- Host computer
 - system requirements 19
- Host machine 218
- Host operating system 218
 - defined 13
- Host-only networking
 - defined 218
 - enabling on Linux host 56
- Hot key preferences 153

I

- IDE
 - drives in virtual machine 26
- Image file
 - floppy 27
 - ISO 26

- Input preferences 151

- Install

- default directories 42, 53
 - on Linux host 50
 - on Windows host 40
 - server software 53
 - silent 47
 - VmCOM API 69
 - VmPerl API 69, 72
 - VMware Management Interface software 58
 - VMware Virtual Machine Console software 64, 67
 - VMware Workstation 37

- Installation

- log 34

- Internationalization 19
- Internet Explorer 6.0
 - and management interface 61

- Inventory
 - defined 218

- ISO image file 26

K

- Kernel
 - reconfiguring GSX Server after Linux kernel upgrade 55

- Keyboard
 - grabbing input 151

- Knowledge base 31

L

- Linux
 - installing on Linux host 50
 - supported guest operating systems 29
 - supported host operating systems 21
 - uninstalling on Linux host 78
 - upgrading on Linux host 84

- Linux host
 - authentication 111
 - authentication daemon 111
 - permissions 111
 - vmware-authd 111

- Localization 19

- Log files 33

M

- Master installer
 - on Windows host 40

- Memory
 - amount required on host 19
 - available in virtual machine 26
 - choosing for best performance 177
 - for all virtual machines 155
 - more than 1GB on a Linux host 188
 - setting size 185

- Migrate
 - disks in undoable mode 171
 - virtual machine 85, 95, 169

- MIME type
 - consoles 157

- Mode
 - full screen 217
 - quick switch 219
- Mouse
 - grabbing input 151
- Move
 - virtual machine 161
- Moving virtual machines
 - UUID 116
- Mozilla
 - MIME type for console 157
- MS-DOS
 - supported guest operating systems 29

N

- NAT
 - defined 218
 - enabling on Linux host 55
- Netscape
 - MIME type for console 157
- NetWare
 - See Novell NetWare
- Network
 - bridged networking 217
 - custom networking 217
 - enabling host-only networking on Linux host 56
 - enabling NAT on Linux host 55
 - host-only 218
 - NAT 218
 - Virtual Network Editor 221
- Network address translation
 - defined 218
- Network Load Balancing
 - clustering 208
- New Virtual Machine Wizard 218
- Newsgroups 31
- Novell Clustering Services
 - clustering 213
- Novell NetWare
 - supported guest operating systems 30

O

- Operating system
 - guest 218

- host 218
- supported guest 29
- supported Linux host 21
- supported Windows host 21

P

- Parallel ports
 - and the Linux kernel 51
- Partition
 - existing 217
- PCI slots
 - in virtual machine 27
 - limits 27
- Performance
 - CD-ROM drive polling 178
 - debugging mode 178
 - disk options 179
 - guest operating system selection 177
 - installing applications in a guest 180
 - memory settings 177
 - memory usage 185
 - remote disk access 180
 - swap space on a Linux host 184
 - temp directory on a Linux host 184
 - using full screen mode on a Linux host 183, 184
- Permissions
 - Linux host 111
 - physical disk 111
 - snapshot 111
 - virtual disks 111
 - virtual machines 106
- Physical disk
 - defined 219
 - permissions 111
- Port numbers
 - console 101
 - management interface 123
- Preferences
 - GSX Server 154
 - hot keys 153
 - input 151
 - keyboard combinations 153
 - shortcut keys 153
 - user 149
 - workspace 149

- Priority
 - preferences 155
 - Windows host 155
- Private
 - virtual machines 107
- Process scheduler
 - Windows host 155
- Processor
 - host requirement 19
 - provided in virtual machine 26
- Q**
- Quick switch mode 219
- Quiet mode
 - install 47
- R**
- RAM
 - amount required on host 19
 - available in virtual machine 26
- Real-time clock
 - requirement on Linux host 51
- Redo log 219
- Registration 31
- Remote management 101
 - encrypted communications 112
 - SSL 112
 - VMware Management Interface 101
 - VMware Scripting APIs 101
 - VMware Virtual Machine Console 101
 - vmware-cmd 101
- Resume
 - defined 219
- S**
- SCSI
 - devices in virtual machine 26
 - generic 119
- SCSI reservation
 - and clustering 192
 - enabling 194
 - issues to consider 196
 - preallocated virtual disks 192
 - sharing SCSI disks 192
 - support 193
- Security certificates
 - custom 113
- Serial number 40
- Set up
 - memory size 185
 - Web browser on Linux host 63
- Shortcut keys
 - configuring 153
- Silent install 47
- SMBIOS
 - modifying UUID 115
- Snapshot
 - defined 220
 - permissions 111
- Specifications
 - virtual machine platform 26
- SSL
 - console connections 112
 - custom security certificates 113
 - enabling 144
 - for consoles 114, 144, 157
 - for the management interface 114
 - management interface connections 112
 - remote management 112
- Support
 - technical support resources 31
- Supported partition 220
- Suspend
 - defined 220
- System requirements 19
 - host server 19
 - remote workstation 23
- T**
- Tools
 - VMware Tools 221
- U**
- Undoable mode
 - migrating 171
- Uninstall
 - on Linux host 78
 - on Windows host 73
- Unsupported partition 220
- Update
 - GSX Server software 150

- Upgrade
 - from GSX Server 1 and 2 79
 - Linux kernel, reconfiguring GSX Server after upgrade 55
 - on Linux host 84
 - on Windows host 83
 - virtual hardware 87
 - virtual machine 85, 95
 - VMware GSX Server 79
- User preferences 149
- UUID 115
 - automatic generation 115
 - modifying 165
 - moving virtual machines 116
 - virtual machine configuration file 116
- V**
- Virtual disk
 - defined 220
 - permissions 111
- Virtual hardware
 - upgrading 87
- Virtual machine
 - accessibility 108
 - backing up 119
 - configuring in management interface 130
 - configuring options in management interface 134
 - configuring virtual hardware 132
 - connected users 139
 - Ctrl+Alt+Delete 153
 - debugging 134
 - default directory 154
 - defined 220
 - deleting from host 142
 - event log 140
 - grabbing input 151
 - heartbeat 128
 - log 33
 - migrating 169
 - moving 161
 - permissions 106
 - platform specifications 26
 - powering off when host shuts down 136
 - powering on when host starts up 136
 - private 107
 - resources and permissions 111
 - running on Linux host 111
 - running on Windows host 108
 - upgrading 85, 95
 - user 108
 - UUID 115
 - VMID 130
- Virtual machine settings editor
 - defined 221
- Virtual Network Editor 221
- VmCOM Scripting API 69
- VmPerl Scripting API 69
- VMware Authorization Service 108
 - log 34
- VMware community forums 31
- VMware guest operating system service
 - virtual machine heartbeat 128
- VMware Management Interface 121
 - advanced configuration options 137
 - Apache commands 141
 - changing port number 123
 - changing virtual machine power state 127
 - configuring to launch console 61
 - configuring virtual hardware 132
 - configuring virtual machines 130
 - connected users 139
 - deleting virtual machines 142
 - disabling SSL 114
 - downloading console installer 104
 - enable JavaScript 123
 - enable style sheets 123
 - enabling SSL 114
 - enabling SSL for remote connections 144
 - encrypted communications 112
 - host summary information 124
 - launching remote console 61
 - launching remote consoles 64
 - log 33
 - logging in 122
 - logging out 141
 - permissions 112
 - proxy servers 62
 - refresh rate 122
 - remote management 101

- VMware Management Interface
 - (continued)
 - run with debugging information 134
 - setting session length 122
 - SSL 112
 - Status Monitor 124
 - supported browsers 122
 - URL to log in 123
 - virtual machine event log 140
 - virtual machine heartbeat 128
 - virtual machine menu 126
 - virtual machine options 134
 - virtual machine summary 124

- VMware Registration Service
 - log 34

- VMware Scripting APIs
 - downloading from management interface 105
 - installing 69
 - remote management 101

- VMware Tools
 - defined 221
 - heartbeat 128

- VMware Virtual Machine Console 221
 - changing port number 101
 - connecting from management interface 125
 - deleting virtual machines 142
 - disabling SSL 114, 144, 157
 - download from management interface 104, 123
 - downloading installer 104
 - enabling SSL 114, 144, 157
 - encrypted communications 112
 - install 64
 - installation 67
 - launching from management interface 61
 - launching from Mozilla 157
 - launching from Netscape 157
 - log 33
 - remote management 101
 - securing connections 157
 - setting MIME type 157
 - SSL 112
 - X server 59

- vmware-authd 111

- vmware-cmd 101
- vmware-config.pl 55
- VNC Viewer
 - using with virtual machines 101

W

- Windows
 - installing on Windows host 40
 - supported guest operating systems 29
 - uninstalling on Windows host 73
 - upgrading on Windows host 83

- Windows 95
 - upgrading guest 98

- Windows 98
 - upgrading guest 96

- Windows host
 - authentication 108
 - configuring permissions 110
 - Event Viewer 117
 - priority preferences 155
 - process scheduler 155

- Windows Me
 - upgrading guest 96

- Windows operating system
 - installing Scripting APIs on 69

- Windows Terminal Services
 - using with virtual machines 101

- Windows XP Remote Desktop
 - using with virtual machines 101

- Wizard
 - new virtual machine 218

- Workspace preferences 149

X

- X server 59
 - required on Linux client 24
 - required on Linux host 22

- XFree86
 - required on Linux client 24
 - required on Linux host 22